



RIVISTA ITALIANA DI INFORMATICA E DIRITTO

PERIODICO INTERNAZIONALE DEL CNR-IGSG

diretta da **Sebastiano Faro • Marina Pietrangelo**

direzione e redazione
Istituto di Informatica Giuridica e Sistemi Giudiziari
Via dei Barucci 20 • 50127 Firenze

anno VI • periodicità semestrale • ISSN 2704-7318

www.rivistaitalianadiinformaticaediritto.it

2•2024

SEZIONI MONOGRAFICHE

*Lo Stato insicuro. Sicurezza e sorveglianza
nella cybersocietà*

a cura di Marina Pietrangelo



*EMFA under the spotlight:
towards a common regulatory framework
to foster media pluralism? - Part 1*

edited by Elda Brogi



Minori e Internet

a cura di

Carlo Colapietro e Antonio Iannuzzi



*Digitalizzazione del processo
e diritti fondamentali. Profili processuali*

a cura di

Francesca Bailo e Michele Francaviglia



*Cittadini e pubbliche amministrazioni
tra AI e diritto all'umano*

a cura di Enrico Carloni



Consiglio Nazionale
delle Ricerche

Organi

DIREZIONE

SEBASTIANO FARO IGSG-CNR
MARINA PIETRANGELO IGSG-CNR

COMITATO DI DIREZIONE

FEDERIGO BAMBI Università di Firenze
ELDA BROGI European University Institute
SIMONE CALZOLAIO Università di Macerata
ENRICO CARLONI Università di Perugia
DAVIDE CARNEVALI IGSG-CNR
GIAN LUCA CONTI Università di Pisa
ENRICO FRANCESCONI IGSG-CNR
ANTONIO IANNUZZI Università Roma-Tre
ERIK LONGO Università di Firenze
LORENZO NANNIPIERI IGSG-CNR
STEFANO PIETROPAOLI Università di Firenze
FRANCESCO ROMANO IGSG-CNR

COMITATO SCIENTIFICO

LAURA ABBA IGSG-CNR
AGATA C. AMATO MANGIAMELI Università di Roma-Tor Vergata
FABIO BRAVO Università di Bologna
ANDREA CARDONE Università di Firenze
ANTONIO CARCATERRA UnitelmaSapienza
PAOLO CARETTI già Università di Firenze
MASSIMO CARLI già Università di Firenze
ELISABETTA CATELANI Università di Pisa
ADRIANA CIANCIO Università di Catania
RENATO CLARIZIA Università Roma-Tre
CARLO COLAPIETRO Università Roma-Tre
GIOVANNI COMANDÉ Scuola Superiore Sant'Anna
GIUSEPPE CORASANITI UnitelmaSapienza
PASQUALE COSTANZO già Università di Genova
GIOVANNA DE MINICO Università di Napoli - Federico II
ROSA MARIA DI GIORGI già IGSG-CNR
ELIO FAMELI già IGSG-CNR
CARLA FARALLI Università di Bologna
GIUSELLA FINOCCHIARO Università di Bologna
TOMMASO E. FROSINI Università di Napoli-Suor Orsola Benincasa
MARIO JORI già Università di Milano
DONATO A. LIMONE UnitelmaSapienza
ALDO LOIODICE Università Europea Roma
LUIGI LOMBARDI VALLAURI già Università di Firenze
NICOLA LUPO Università di Roma-LUISS
NICOLETTA MARASCHIO Accademia della Crusca
PAOLA MARSOCCI Università Roma-Sapienza
GAETANA MORGANTE Scuola Superiore Sant'Anna
PAOLO MORO Università di Padova
MONICA PALMIRANI Università di Bologna
UGO PAGALLO Università di Torino
GIOVANNI PASCUZZI Consiglio di Stato
PAOLO PASSAGLIA Università di Pisa
ORESTE POLLICINO Università di Milano-Bocconi

BENEDETTO PONTI Università di Perugia
GIOVANNI SARTOR Università di Bologna
ANDREA SIMONCINI Università di Firenze
CARLO SORRENTINO Università di Firenze
GIANCARLO TADDEI ELMI già IGSG-CNR
LARA TRUCCO Università di Genova
STEFANO TRUMPY Internet Society Italia
ALESSANDRA VALASTRO Università di Perugia
FRANCO VALLOCCHIA Università Roma-Sapienza
GIOVANNI ZICCARDI Università di Milano

ESPERTI PER LA VALUTAZIONE

FULVIA ABBONDANTE Università di Napoli-Federico II
ENRICO ALBANESI Università di Genova
MARIA ROMANA ALLEGRI Università Roma-Sapienza
ROSANNA AMATO IGSG-CNR
SIMONE BARBARESCHI Università Roma-Tre
MARCO BASSINI Tilburg University
BRUNO BRANCATI Università di Pisa
RAFFAELLA BRIGHI Università di Bologna
GIUSEPPE CAMMAROTA Università di Cagliari
FRANCESCO CAMPIONE Università di Padova
GIANLUIGI CIACCI Università di Roma-LUISS
SOFIA CIUFFOLETTI Università di Firenze
GUIDO COLAIACOVO Università di Foggia
ALFONSO CONTALDO Accademia di Belle Arti di Roma
MELANIA D'ANGELOSANTE Università "G. D'Annunzio" di Chieti e Pescara
SUSANA DE LA SIERRA Universidad de Castilla-La Mancha
GABRIELLA DE MAIO Università di Napoli-Federico II
MARIA VITTORIA DELL'ANNA Università del Salento
FABIO DELL'AVERSANA Accademia di Belle Arti di Napoli
FRANCESCO DI CIOMMO Università di Roma-LUISS
STEFANO DORIGO Università di Firenze
ROSSANA DUCATO Università di Trento
MARIA SAMANTHA ESPOSITO Politecnico di Torino
FERNANDA FAINI Università Telematica Pegaso
PIETRO FALLETTA Università dell'Insubria
GIANLUCA FASANO ISTC-CNR
CHIARA FAVILLI Università di Firenze
ANGELA MARIA FELICETTI Università di Bologna
GAIA FIORINELLI Scuola Superiore Sant'Anna
ROBERTO FLOR Università di Verona
SIMONE FRANCA Università di Trento
ELISABETTA FRONTONI Università Roma-Tre
RAFFAELE GALARDI Università di Pisa
PAOLO GALDIERI Università di Napoli-Federico II
GIOVANNI GALLONE Consiglio di Stato
MATTEO GIANNELLI Università di Firenze
ANDREA GIUBILEI Università Roma-Tre
OTTAVIO GRANDINETTI Università di Napoli-Suor Orsola Benincasa
RICCARDO GUALDO Università della Toscana
PAOLO GUARDA Università di Trento
RENATO IBRIDO Università di Firenze
ILARIA KUTUFÀ Università di Pisa

NICOLE LAZZERINI Università di Firenze
ANTONELLO LO CALZO Università di Pisa
ALESSANDRO LOVARI Università di Cagliari
ALESSANDRO M. LUCIANO Università di Firenze
GIANCLAUDIO MALGIERI Free University of Brussels - VUB
CARLO MARCHETTI Senato della Repubblica
ISAAC MARTÍN DELGADO Universidad de Castilla-La Mancha
FABIO MARTINELLI IIT-CNR
DANIELE MARONGIU Università di Cagliari
LETIZIA MATERASSI Università di Firenze
MARIO MAURO Università di Firenze
HAIDEER MIRANDA BONILLA Università del Costa Rica
GIUSEPPE MOBILIO Università di Firenze
MATTEO MONTI Università di Roma-LUISS
IVAN LIBERO NOCERA Università di Bergamo
ANGELO GIUSEPPE OROFINO Università LUM
VALENTINA PAGNANELLI Università di Firenze
ERICA PALMERINI Scuola Superiore Sant'Anna
SAULLE PANIZZA Università di Pisa
ANNA PAPA Università di Napoli-Parthenope
VIVIANA PATTI Università di Torino
MARIA GRAZIA PAZIENZA Università di Firenze

GIORGIO PEDRAZZI Università di Brescia
NICOLA PETTINARI Università di Perugia
GIOVANNI PICCIRILLI Università di Roma-LUISS
EDOARDO RAFFIOTTA Università di Milano-Bicocca
FEDERICO NICCOLÒ RICOTTA IGSG-CNR
CECILIA ROBUSTELLI Università di Modena e Reggio Emilia
MONICA ROSINI Libera Università di Bolzano
ANDREA ROSSETTI Università di Milano-Bicocca
SILVIA SALARDI Università di Milano-Bicocca
SILVIA SASSI Università di Firenze
SIMONE SCAGLIARINI Università di Modena e Reggio Emilia
FEDERICO SERINI Università Roma-Sapienza
CATERINA SGANGA Scuola Superiore Sant'Anna
MAURIZIO TESCONI IIT-CNR
MARCO TORRE Università di Firenze
EMILIO TOSI Università di Milano-Bicocca
GIUSEPPE VACIAGO Università dell'Insubria
GIULIA VENTURI ILC-CNR
CATERINA VERRIGNI Università "G. D'Annunzio" di Chieti e Pescara
ELENA VIVALDI Scuola Superiore Sant'Anna
PAOLO ZUDDAS Università degli Studi dell'Insubria

Con la pubblicazione della nuova *Rivista italiana di informatica e diritto*, l'IGSG-CNR prosegue l'attività editoriale avviata nel 1972 con la pubblicazione prima del *Bollettino bibliografico d'informatica generale e applicata al diritto* e poi, dal 1975, della rivista *Informatica e diritto* nata come organo dell'allora Istituto per la Documentazione Giuridica (IDG-CNR), poi diventato Istituto di Teoria e Tecniche dell'Informazione Giuridica (ITTIG-CNR), confluito ora nell'IGSG-CNR.

Al momento della sua nascita, nel 1975, l'aspirazione dei promotori della rivista *Informatica e diritto* era di «iniziare in Italia un discorso critico, scientificamente fondato, sull'informatica e sui rapporti di questa nuova disciplina e realtà sociale col diritto» con la convinzione di «colmare il vuoto culturale esistente nel panorama delle riviste italiane e, in particolare, di quelle giuridiche» (così si legge nella presentazione firmata dal comitato direttivo formato da Luigi Lombardi Vallauri, Mario G. Losano e Costantino Ciampi). La Rivista mirava a rispondere alla «esigenza di un approccio all'informatica da parte del giurista che fosse unitario e non più separato per sfere di interesse», secondo un modello che andava emergendo in altri Paesi, continuando l'esperienza già avviata nel 1972 con il *Bollettino bibliografico d'informatica generale e applicata al diritto*.

Nell'arco di oltre quarant'anni *Informatica e diritto* ha ampiamente realizzato le funzioni che per essa intravedevano i suoi promotori. Con funzione informativa, essa ha fatto conoscere ai lettori idee, problemi e fatti del mondo dell'informatica giuridica e del diritto dell'informatica, dando conto anche dello sviluppo delle ricerche in un settore allora emergente e delle prospettive – non solo giuridiche, ma anche politiche e sociali – a esso collegate. Con la non meno importante funzione di approfondimento scientifico, promozione e coagulo di ricerche specialistiche e settoriali la Rivista ha dato spazio a idee e riflessioni che hanno avuto un ruolo significativo nella evoluzione dell'informatica giuridica in Italia e all'estero. Alcuni saggi pubblicati in *Informatica e diritto* sono ancora oggi autentiche pietre miliari nella storia dell'informatica giuridica e del diritto dell'informatica, a testimonianza dell'importanza e dell'impatto che essa ha avuto nel dibattito scientifico sui temi del rapporto fra diritto e tecnologie dell'informazione e della comunicazione.

Nel 2019, l'Istituto di Informatica Giuridica e Sistemi Giudiziari (IGSG) ha aperto una nuova pagina nella storia della sua rivista, affidata adesso alla Rete nell'ottica di una politica di accesso aperto alle pubblicazioni scientifiche (secondo il modello del "Diamond Open Access"): è nata, quindi, la *Rivista italiana di informatica e diritto* che rappresenta il diretto proseguimento di *Informatica e diritto* da cui eredita il programma scientifico, l'approccio e l'ampia apertura alla realtà internazionale, oltre che i componenti degli organi scientifici, arricchiti di nuove personalità scientifiche rispetto alla formazione originaria.

SEGRETERIA DI REDAZIONE Simona Binazzi e Mariasole Rinaldi
ELABORAZIONE TESTI E GRAFICA Giuseppina Sabato e Teresa Balsamo
RESPONSABILE DEL SITO WEB Elisabetta Marinai

DIREZIONE E REDAZIONE

IGSG/CNR • Via dei Barucci, 20 • 50127 Firenze
Tel. +39 055 43995 • rivistaRIID@igsg.cnr.it • www.rivistaitalianadiinformaticaediritto.it

DIRETTORE RESPONSABILE

Sebastiano Faro • Registrazione presso il Tribunale di Roma al n. 127/2019

Indice

Sezioni monografiche

Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà

a cura di Marina Pietrangelo

Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà. Introduzione [MARINA PIETRANGELO]	11
La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo [MARINA PIETRANGELO]	13
Dalla sorveglianza al controllo: la parabola della governamentalità algoritmica [STEFANO PIETROPAOLI]	25
Metaverso, <i>Digital Twins</i> e diritti fondamentali [ANTONIO IANNUZZI]	35
Il rapporto tra cybersicurezza e tutela dei dati personali: sinergie, bilanciamenti e parallelismi [BENEDETTO PONTI]	57
Cybersicurezza e protezione dati: un rapporto ambivalente [FEDERICA RESTA]	67
Cybersicurezza e appalti. Interventi legislativi e prime criticità [LORENZO NANNIPIERI]	71
<i>Vulnerability disclosure e penetration testing</i> : profili giuridici rilevanti per l'adozione di una politica nazionale conforme alla Direttiva NIS 2 [FEDERICO NICCOLÒ RICOTTA]	81
Strategie e modelli operativi per la sicurezza delle pubbliche amministrazioni al tempo del PNRR [INDRA MACRÌ]	93
Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano [MILENA ANTONELLA RIZZI, FEDERICO SERINI]	115

EMFA under the spotlight: towards a common regulatory framework to foster media pluralism? - Part 1

a cura di Elda Brogi

EMFA under the spotlight: towards a common regulatory framework to foster media pluralism? Introduction [ELDA BROGI]	139
Quale nozione di pluralismo nell'EMFA? [OTTAVIO GRANDINETTI]	143
La valutazione delle concentrazioni per la tutela del pluralismo informativo [ANTONIO MANGANELLI, MARIA LUCE MARINIELLO]	159
From rhetoric to regulation: EMFA and media concentration in the digital age [TANJA KERŠEVAN]	173
Safeguards for the independent functioning of public service media providers. The legal position of domestic legislation that is not in compliance with Article 5 EMFA [ENRICO ALBANESI]	187
The missing piece in the DSA puzzle? Article 18 of the EMFA and the media privilege [MATTEO MONTI]	195
DSA e EMFA: speciale responsabilità delle piattaforme online e tutela della libertà dei media [LILIANA CILIBERTI]	213

Media ownership transparency and the European Media Freedom Act: how did the EU get there? [DANIELLE BORGES]	259

Digitalizzazione del processo e diritti fondamentali – Profili processuali

a cura di Francesca Bailo e Michele Francaviglia

Digitalizzazione del processo e diritti fondamentali – Profili processuali. Introduzione [FRANCESCA BAILO, MICHELE FRANCAVIGLIA]	269
AI Act e consulenza legale online: problemi in tema di accesso alla giustizia [PAOLO COMOGLIO]	273
Riforma Cartabia e digitalizzazione della giustizia penale [JACOPO DELLA TORRE, ALESSANDRO MALACARNE]	287
Diritto di difesa, accesso a Internet rimozione degli “ostacoli di ordine economico e sociale” [SIMONE CAFIERO]	317

Minori e Internet

a cura di Carlo Colapietro e Antonio Iannuzzi

I diritti dei minori nella società digitale tra profili di responsabilità ed esigenze di protezione [CARLO COLAPIETRO, ANTONIO IANNUZZI]	333
La tutela dei minori nel prisma della protezione dei dati personali. I sistemi di verifica dell'età tra personalismo ed esigenze di bilanciamento fra diritti [SIMONETTA TROZZI]	339
L'identità e l'identificazione digitale del minore tra normativa nazionale e internazionale e i provvedimenti delle autorità competenti [FRANCESCA RICCIULLI]	355
Protezione dei minori dai contenuti nocivi circolanti sulle <i>Video Sharing Platforms</i> : un'ipotesi di (ir)ragionevolezza legislativa? [GIOVANNI BAROZZI REGGIANI]	371
<i>Sharenting</i> e tutela dei dati personali del minore: profili giuridici di un fenomeno interdisciplinare [DORINDA CACCIOPPO]	385
Minori su Internet: profili di responsabilità [DOMIZIANO PIERANTONI]	399
Autonomia e controllo dei minori on line. I nuovi confini della responsabilità genitoriale [BENEDETTA AGOSTINELLI]	415
Strumenti di <i>age verification</i> alla luce del contributo del Garante privacy e dell'AGCOM: il rischio di obsolescenza tecnologica e conoscitiva [LORENZO MARIA LUCARELLI TONINI]	435

Cittadini e pubbliche amministrazioni tra AI e diritto all'umano

a cura di Enrico Carloni

Dalla legalità algoritmica alla legalità (dell'amministrazione) artificiale. Premesse ad uno studio [ENRICO CARLONI]	451
<i>Human in the loop</i> . L'essere umano come fattore condizionante della – o condizionato dalla – intelligenza artificiale [DARIO MARTIRE]	467
Strumenti informatici nel processo decisionale amministrativo ed effettività del diritto di difesa: questioni vecchie e problemi nuovi alla luce del Regolamento (UE) 2024/1689 [CRISTINA NAPOLI]	483
La prospettiva dell'intelligenza artificiale nel procedimento e nell'attività amministrativa [ILDE FORGIONE]	505
Il fornitore dell'algoritmo quale soggetto estraneo all'amministrazione [BENEDETTO PONTI]	517
La <i>data science</i> come nuovo sapere per governare le intelligenze artificiali nelle pubbliche amministrazioni [MATTEO FALCONE]	527

Studi e ricerche

Predictive algorithms and criminal justice: expectations, challenges and a particular view of the Spanish VioGén system [PILAR MARTÍN RÍOS]	547

L'interpretazione estensiva della nozione di "decisione automatizzata" ad opera della Corte di giustizia: una prospettiva più ampia ma ancora fragili tutele per le libertà fondamentali [GIANLUCA FASANO]	563
Intelligenza artificiale in medicina: alcune risposte – significative, ma parziali – offerte dal codice di deontologia medica (in materia di non discriminazione, consenso informato e relazione di cura) [PAOLO ZUDDAS]	579
Nuove prassi e norme per un sistema sanitario "smart": ricadute dell'AI Act sulla relazione di cura [TONINO CANTELMÌ, LUISA LODEVOLE]	607
<i>Ne pereant fragmenta: l'intelligenza artificiale e la complessità della Corptech governance</i> [RICCARDO MICHELE COLANGELO]	631

Sistemi e applicazioni

<i>Missing Trader Ontology</i> (MTO): un'ontologia per il rilevamento delle società cartiere e la prevenzione delle frodi all'IVA intracomunitaria [MATTEO LONGO]	645

Note e discussioni

The state of the art of the Brazilian Bill on Artificial Intelligence with a focus on civil responsibility [VINCENZO CALDERONIO]	679
Cybersecurity e sovranità digitale nella protezione dei dati personali [ELISA SORRENTINO, ANNA FEDERICA SPAGNUOLO]	685

Osservatori

Sviluppi recenti in tema di Intelligenza Artificiale e diritto. Una rassegna di legislazione, giurisprudenza e dottrina (maggio-ottobre 2024) [GIANCARLO TADDEI ELMÌ, SOFIA MARCHIAFAVA]	703

Recensioni

Recensione a: Paola Lucarelli (a cura di), <i>Giustizia sostenibile. Sfide organizzative e tecnologiche per una nuova professionalità</i> , Firenze, University Press, 2023 [MARCO FABRI]	723

Autori del 2024	729

Sezione monografica

Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà

a cura di
Marina Pietrangelo



RIVISTA ITALIANA DI
INFORMATICA E DIRITTO

PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0201 • articolo sottoposto a peer review • pubblicato in anteprima il 20 dic. 2024
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale 

MARINA PIETRANGELO

Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà

Introduzione

L'Autrice è prima ricercatrice presso l'Istituto di Informatica Giuridica e Sistemi Giudiziari del CNR

Questo contributo fa parte della sezione monografica *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà*, a cura di Marina Pietrangelo

I'm the creeper, catch me if you can!

La cybersicurezza è oggi una questione di democrazia. Si tratta di un'affermazione che fino a pochi decenni fa sarebbe parsa eccentrica, specie se intestata a una raccolta di approfondimenti giuridici. Eppure essa esprime esattamente il tratto comune dei lavori pubblicati in questa Sezione monografica, che riflettono – pur se da angolazioni differenti – sulla “gestione” delle attività di protezione di reti, sistemi e dati in termini di tutela dei diritti fondamentali, garanzie del potere costituito, ruolo delle istituzioni pubbliche e produzione normativa. In pochi decenni abbiamo assistito alla comparsa dei primi virus informatici e alla successiva diffusione di virus malevoli, strumenti di attacco via via più potenti, allo sviluppo e al consolidamento di misure reattive di sicurezza informatica sempre più specializzate: veri e propri apparati di attacco e difesa. In questo contesto, altrettanto rapidamente la cybersicurezza esce dai laboratori informatici e diventa “faccenda di Stato”, entrando a pieno titolo nelle agende istituzionali di governi, regolatori, giudici, amministrazioni pubbliche.

Molte sono, dunque, le questioni in evidenza; e molti gli interrogativi su cui insistono i saggi di questa sezione. Di grande interesse è ancora il tema della relazione tra interessi giuridici diversi, e precisamente tra protezione dei dati personali e protezione della sicurezza pubblica cibernetica, che non pare aver ancora trovato una stabile declinazione (Resta, Ponti). Parimenti aperta è la riflessione sull'impatto che la combinazione di tecnologie più recenti (blockchain, applicazioni basate su IA ecc.) potrà avere sul godimento dei diritti fondamentali (Iannuzzi) e sulla complessiva tenuta dei sistemi democratici (Pietropaoli). In questo contesto ancora “sotto osservazione” un dato è però certo: la regolazione è già ipertrofica. L'obiettivo di introdurre misure sempre più stringenti di prevenzione e repressione degli attacchi informatici rivolti alla collettività, ai singoli, alle aziende, alle amministrazioni pubbliche tradisce un eccesso di fiducia in un sistema di regole che per il vero risulta già di dubbia o difficile applicazione (Macrì, Nannipieri) e che – per la rilevanza odierna della “materia” – sta ridisegnando anche la mappa dei poteri digitali (Rizzi-Serini, Pietrangelo, Ricotta).

A conclusione di questa breve nota introduttiva vorrei scrivere qualche riga di sincero ringraziamento. Anzitutto alle autrici e agli autori, amiche e amici, che hanno accettato di condividere questo piccolo (ma robusto, grazie a loro) approfondimento, con scritti di grande attualità e, ne sono certa, di rilievo per la discussione scientifica.

Un secondo ringraziamento a chi ha materialmente realizzato l'opera, per la cura, la precisione, la disponibilità e la passione mai scontate: Simona Binazzi, Giuseppina Sabato e Elisabetta Marinai.

Questa Sezione monografica è parzialmente supportata dalle attività del progetto *SEcurity and RIghts in the CyberSpace* (MUR PNRR).



RIVISTA ITALIANA DI
INFORMATICA E DIRITTO

PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0196 • articolo sottoposto a peer review • pubblicato in anteprima il 19 dic. 2024
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale 

MARINA PIETRANGELO

La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo

Il saggio esamina criticamente alcuni aspetti dell'attuale assetto di governo della cybersicurezza. Muovendo da una ridefinizione estensiva del concetto, si prospettano una maggiore valorizzazione degli interventi di carattere sociale e un rafforzamento delle azioni istituzionali di controllo e collaborazione.

*Profili giuridici della cybersicurezza – Governo della cybersicurezza – Governance digitale
Dimensione sociale della cybersicurezza*

The plural dimension of cybersecurity: from invisible power to collaborative process

The paper critically examines some aspects of the current cybersecurity's legal framework. The concept of cybersecurity is extensively redefined to highlight some critical issues. The main demand is for social measures and forms of institutional control and cooperation.

Legal aspects of cybersecurity – Cybersecurity government – Digital governance – Cybersecurity awareness

L'Autrice è prima ricercatrice presso l'Istituto di Informatica Giuridica e Sistemi Giudiziari del CNR

Questo contributo fa parte della sezione monografica *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà*, a cura di Marina Pietrangelo

SOMMARIO: 1. Premessa. La cybersicurezza come “condizione di esistenza” della digitalizzazione. – 2. Il modello politico-amministrativo nazionale di cybersicurezza: coordinamento o accentramento. – 2.1. I settori interrelati con la funzione di cybersicurezza. – 3. Per concludere, con alcuni interrogativi.

1. Premessa. La cybersicurezza come “condizione di esistenza” della digitalizzazione

Negli ultimi decenni la governance del digitale ha polarizzato il dibattito pubblico e la riflessione scientifica. Sono stati censiti e analizzati diversi modelli di gestione e governo dello spazio digitale; e ne sono stati proposti di nuovi, spesso con l'obiettivo di appianare o risolvere sbilanciamenti e contrasti già consolidati tra poteri pubblici e poteri privati¹. La digitalizzazione pervasiva e totalizzante, benché ancora “in transito”, ha infatti travolto e mutato non soltanto gli stili di vita delle persone nella loro quotidianità professionale e di relazione, ma anche gli apparati delle istituzioni e la declaratoria delle relative loro funzioni². Nuove autorità

con nuovi poteri richiesti dalla mole di incombenze connesse agli usi delle tecnologie digitali sono subentrate nella mappa di poteri preesistente, affiancandoli, talvolta sovrappponendosi ad essi, tal altra guadagnando in modo non sempre trasparente porzioni rilevanti di capacità decisionale. L'esigenza di fare presto per supportare la decisiva transizione digitale e assicurare alla collettività un'adeguata protezione dagli abusi di cui i processi di digitalizzazione pure sono costellati ha di fatto finito per esautorare le sedi della rappresentanza e del controllo, in favore di una supposta maggiore efficienza della decisione governativa: un modello verticale di esercizio del potere pubblico digitale, che tradisce però l'idea di una sovranità digitale tutta imperniata sulle misure tecniche di cybersicurezza e scollegata dalla sua dimensione sociale.

1. Per uno sguardo d'insieme, v. BRADFORD 2023, che mette bene a fuoco i tre diversi modelli di governo del digitale (Usa, Cina e Ue) e SORO 2019; FINOCCHIARIO–BALESTRA–TIMOTEO 2022; e volendo, ABBA–LAZZARONI –PIETRANGELO 2022. Sul “rapporto tra poteri”, v. in particolare TORCHIA 2024; POLLICINO 2023, pp. 410 ss.; RESTA 2023, p. 1008 ss.; FERRARESE 2022; BETZU 2021. Sulle evoluzioni delle categorie oggettive e soggettive del diritto contemporaneo, non soltanto in relazione ai poteri e al governo dello spazio digitale, v. ampiamente ZACCARIA 2022, che individua nella coppia “destrutturazione-pluralismo” la chiave di lettura delle modificazioni dell'ordine giuridico contemporaneo. La prima formula indicherebbe l'insieme di fattori di crisi e di alterazione dell'assetto giuridico tradizionale, i cui soggetti, strumenti ed enti «sono costretti a continuare le loro funzioni pur in un quadro ampiamente e strutturalmente mutato» (p. 13). Il secondo termine della coppia vorrebbe rappresentare l'apertura pluralistica «alla presenza e all'azione di un maggior numero di soggetti, pubblici e privati» (*ivi*).
2. Così FERRARESE 2022, *passim*, la quale analizza due distinti fenomeni di mutamento del quadro dei poteri negli ultimi anni del Novecento significativamente condizionati dallo sviluppo tecnologico: il “trasloco” del potere, che non abita più «necessariamente solo in palazzi governativi e statali, con note etichette ufficiali, ma ha trovato nuove residenze sia in sedi internazionali, sia specialmente in sedi private, smettendo di indossare i consueti abiti istituzionali sotto l'egida del diritto pubblico» (p. 9); e la sua “metamorfosi”, cioè un mutamento nel «modo di essere e di presentarsi» (*ibidem*), che è ravvisabile nella «diffusa tendenza a ri-forgiare le modalità e le forme di potere, producendo misture, travasi e confluenze di vario tipo, nonché creando nuovi canali di scorrimento spesso di tipo orizzontale» (*ibidem*). Sul punto, v. anche ZACCARIA 2022, specie p. 37 ss.

Si tratta di modificazioni “strutturali” del nostro ordinamento costituzionale che paiono andar ben al di là di quanto previsto dal dettato normativo, aprendo nuovi fronti in una crisi istituzionale ancora irrisolta, per molta parte occasionata proprio dall’erompere di nuovi “poteri tecnologici”³.

Occorre allora interrogarsi sugli effetti, oltre che sulle intuibili ragioni, di questo disegno istituzionale, alla ricerca di correttivi e interventi capaci di riportare l’esercizio del potere pubblico nell’alveo di un sistema rappresentativo nel quale le misure di controllo e partecipazione recuperino il legittimo spazio sul protagonismo assoluto degli apparati governativi. Ciò anche in ragione della continua erosione del circuito della rappresentanza, già di per sé svilito da una produzione normativa frammentata e mossa da contingenze o stati emergenziali (oggettivi o dichiarati)⁴.

Parallelamente, occorre coltivare un approccio estensivo alla cybersicurezza, che ne valorizzi in modo permanente la dimensione sociale – e

dunque le misure di carattere educativo-formativo, sociale e sanitario – tutte decisive per elevare il grado complessivo di sicurezza del Paese (cosiddetta *cyber security awareness*)⁵. Agendo su entrambi i fronti, cioè maggiore controllo sugli apparati governativi e rafforzamento della collaborazione tra enti per attivare misure sociali diffuse, si conterrebbe l’espansione senza contrappesi di un nuovo potere, che sembra farsi sempre più assoluto e invisibile⁶.

2. Il modello politico-amministrativo nazionale di cybersicurezza: coordinamento o accentramento

La definizione normativa che ricorre nella fitta e stratificata regolazione in materia, funzionale anzitutto all’applicazione di obblighi di adeguamento o ripristino delle misure minime di sicurezza informatica, pure se necessaria, risulta oggi riduttiva sotto il profilo concettuale⁷. Essa, infatti, riconduce la cybersicurezza nell’alveo primigenio della

3. Ben evidenzia le molte questioni poste dall’erompere del potere tecnologico nell’ordinamento costituzionale SIMONCINI 2022, pp. 133-154, il quale ritiene che vadano indagate con un nuovo approccio «“ibrido”, capace cioè di utilizzare diverse forme di propulsione, così come un linguaggio e un metodo di analisi comprensibili sia dal regolatore che dal regolato» (p. 147). E al riguardo, a proposito della regolazione delle applicazioni di intelligenza artificiale, suggerisce due vie da esplorare, attingendo al diritto privato della concorrenza e al diritto amministrativo. Per il caso specifico della cybersicurezza, v. VEDDER 2019, p. 11 ss.

4. Sul punto, v. le considerazioni recenti di STAIANO 2024.

5. V. al proposito il rilievo assegnato dal National Cyber Security Center dell’UK alla “cyber hygiene” e alle azioni collettive: «(...) Defending the UK’s democratic institutions and processes is a priority for the NCSC. However, it is not something we can achieve alone. It requires a collective effort across the whole of society, including industry and in partnership with allies, to defend our values and make the UK an unattractive environment for hostile actors. Our democracy is founded on the principle of participation; every member of the public across the four nations of the UK has a stake, and everyone has a role to play in defending it.» (NCSC Annual Review 2023, p. 41). Il tema della consapevolezza è oggi sempre più decisivo, visto anche l’aumento negli ultimi mesi di attacchi sofisticati che riescono ad aprire una backdoor sui sistemi delle vittime senza bisogno di alcuna interazione. Mediante la tecnica del *drive-by-compromise* l’utente-vittima naviga su un browser vulnerabile che lo indirizza su un sito fake, cioè su un social engineering che ridistribuisce URL malevoli. Cfr. il caso recente dei RomCom RAT, su cui LAKSHMANAN 2024. Sull’approccio “olistico” alla cybersicurezza, v. ampiamente le attività del progetto PNRR SERICS (*Security and Rights in CyberSpace*), finanziato dall’Unione europea nel programma NextGenerationEU, cui sono in parte riconducibili le riflessioni sviluppate in questa Sezione monografica.

6. Sulla rilevanza della collaborazione, v. ampiamente BALDONI 2024.

7. Secondo la definizione del DPCM 17 febbraio 2017 la cybersicurezza è l’insieme di «idonee misure di sicurezza fisica, logica e procedurale rispetto ad eventi, di natura volontaria od accidentale, consistenti nell’acquisizione e nel trasferimento indebito di dati, nella loro modifica o distruzione illegittima, ovvero nel danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi». Con la direttiva UE 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell’Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la

normazione tecnica settoriale, entro cui sono nate e sono state elaborate le prime definizioni di cybersecurity, computer security e information security⁸. Con la massiva penetrazione sociale delle applicazioni digitali, la sicurezza informatica intesa come sicurezza di sistemi, reti e dati a fini di protezione da abusi e manomissioni ha registrato tuttavia una vera e propria estensione semantica, in ragione della quale essa è oggi ricondotta alle attività di sicurezza pubblica preordinate alla protezione degli interessi nazionali, alla stabilità delle istituzioni e all'ordinato vivere civile⁹. Per conseguenza, l'attribuzione di compiti e funzioni in materia di cybersicurezza ha coinciso con la relativa declaratoria costituzionale e normativa. Nel contesto geopolitico e socio-economico attuale sta invero emergendo e consolidandosi una ulteriore evoluzione del concetto, in cui al profilo già consolidato della sicurezza (informatica) pubblica come insieme di misure di protezione dell'interesse nazionale si sono addentellati nuovi ambiti connessi e interrelati, per nulla secondari, che anzi irrobustiscono la cybersicurezza come processo, chiamando in causa con sempre maggiore urgenza altri attori istituzionali. Si pensi alla sfera della organizzazione e gestione autonoma dei patrimoni informativi

pubblici o ai servizi pubblici online erogati dagli enti territoriali: tutti beni o servizi digitali dei quali occorre garantire la sicurezza, assicurandone la continuità, col fine ultimo di tutelare i diritti degli "utenti"¹⁰. In uno scenario socio-economico sempre più complesso, non pare per esempio sufficientemente esplorata l'opportunità di «sistematizzare un canale di comunicazione/collaborazione stabile tra il livello nazionale e quello regionale/locale, affinché i territori interessati vengano prontamente allertati»¹¹ o di coinvolgere stabilmente i diversi livelli di Governo, attraverso il sistema delle conferenze o mediante la costituzione di una specifica nuova sede istituzionale. Un coinvolgimento diretto che favorirebbe peraltro la condivisione di processi già avviati o consolidati (si pensi per esempio ai percorsi di *Security Awareness Training*) e di non ripetere gli errori del passato in tema di digitalizzazione, evitando cioè approdi disomogenei e non condivisi. Come noto, uno dei fattori di maggior successo degli attacchi informatici rivolti ai sistemi delle amministrazioni pubbliche locali è proprio la tardiva digitalizzazione, spesso non corredata di adeguate misure formative.

Se dunque gli attacchi informatici sono una "questione di interesse pubblico"¹², l'interesse

direttiva (UE) 2016/1148 (cosiddetta NIS 2, recepita in Italia col d.lgs. 4 settembre 2024, n. 138), le misure di gestione dei rischi devono ora comprendere azioni tecniche, ma anche operative e organizzative (cfr. l'art. 21 della direttiva), secondo un approccio cosiddetto "multirischio".

8. Così RIZZI-SERINI 2024, specie p. 7 ss., cui si rinvia per una più ampia ricostruzione del percorso di transito e ingresso – dalla normazione tecnica agli ordinamenti giuridici – dei concetti su richiamati.
9. Corte costituzionale 14 giugno 1956, n. 2: «Esclusa l'interpretazione, inammissibilmente angusta, che la "sicurezza" riguardi solo l'incolumità fisica, sembra razionale e conforme allo spirito della Costituzione dare alla parola "sicurezza" il significato di situazione nella quale sia assicurato ai cittadini, per quanto è possibile, il pacifico esercizio di quei diritti di libertà che la Costituzione garantisce con tanta forza. Sicurezza si ha quando il cittadino può svolgere la propria lecita attività senza essere minacciato da offese alla propria personalità fisica e morale; è l'"ordinato vivere civile", che è indubbiamente la meta di uno Stato di diritto, libero e democratico.» (Diritto, n. 5).
10. Sulla dimensione giuridica della sicurezza pubblica, v. ampiamente MOSCA 2021; URSI 2022; URSI 2023.
11. Cfr. sul punto Conferenza unificata 8 luglio 2021 (rep. atti. n. 70), Parere, ai sensi dell'articolo 9 del decreto legislativo 28 agosto 1997, n. 281, sul decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionali.
12. *Ibidem*. Su questa linea v. la recente l.r. Regione Toscana 9 dicembre 2024, n. 57 recante *Disciplina dell'innovazione digitale nel territorio regionale e tutela dei diritti di cittadinanza digitale. Modifiche alla l.r. 54/2009*.
13. Cfr. il Considerando 1 del regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio del 23 ottobre 2024 relativo a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza), ove si legge «Gli attacchi informatici costituiscono una *questione di interesse pubblico* dal momento che hanno

pubblico alla cybersicurezza non può che essere interesse *della e per la* collettività, un obiettivo ambizioso perseguibile mediante azioni di cybersicurezza tecnico-economica accompagnate e mai disgiunte da misure preventive continue e capillari di cultura della sicurezza informatica¹³. Occorre cioè considerare come immanenti e necessarie – e non suppletive o di corredo – per la resilienza cybernetica le misure di carattere educativo-formativo e socio-sanitario: esse sole possono infatti elevare il grado di cybersicurezza del Paese in termini di consapevolezza a livello individuale o di ente. Una dimensione plurale della cybersicurezza cui deve corrispondere una molteplicità di azioni, funzionali a valorizzare sia la soluzione tecnica sia il fattore umano (e con esso il “fattore sociale”)¹⁴.

D'altro canto, proprio le modificazioni istituzionali occasionate dall'urgenza di governare e regolare le evoluzioni tecniche più di altre paiono scavare carsicamente nell'ordinamento costituito. Corrono cioè sottotraccia mutamenti che paiono andare ben al di là delle attribuzioni normative di

nuove funzioni e nuovi compiti; e che richiamano alla mente il tema della visibilità del potere¹⁵. È grande cioè il sospetto che la cybersicurezza si identifichi oggi in un potere molto specializzato e poco visibile, malcelato sotto le vesti riabilitative di un decisore pubblico che suo tramite punta a recuperare la primazia nella complessa mappa dei poteri digitali¹⁶. Certo è che nelle politiche e pratiche della transizione digitale la cybersicurezza è oggettivamente una condizione di esistenza: rendere più sicuri reti, sistemi e dati vuole dire gioco forza rendere più sicuri gli Stati e i loro apparati, le persone e le loro vite. Una specie di protezione delle protezioni, una sicurezza maxima da cui dipendono le sorti delle Nazioni come degli individui, tutti inesorabilmente immersi nella dimensione digitale: la rilevanza democratica della gestione della cybersicurezza non pare dunque più in discussione¹⁷. Anzi, essa è oggi divenuta quasi uno strumento di “riscossa” degli Stati e del potere pubblico, che con essa tornano simbolicamente a farsi salvifici proprio a garanzia degli interessi della collettività che si muove nello spazio digitale¹⁸.

un impatto determinante non solo sull'economia dell'Unione, ma anche *sulla democrazia*, nonché sulla sicurezza dei consumatori e sulla salute.» (corsivi aggiunti). Gli attacchi informatici aumentano costantemente. Secondo il Rapporto Clusit 2024, nel primo semestre 2024 gli attacchi sono «cresciuti del 23% rispetto al semestre precedente. In media, si sono verificati nel mondo 9 attacchi importanti al giorno; in Italia il 7,6% degli incidenti. La sanità è il settore più colpito a livello globale. In Italia bersagliato il manifatturiero, ma gli attacchi alla sanità crescono dell'83% rispetto al primo semestre 2023» (cfr. CLUSIT 2024, p. 7).

13. Distingue tra nozione estesa di cybersicurezza, che interessa il livello socio-cognitivo – cioè l'insieme delle relazioni umane –, e nozione ristretta, che invece riguarda la protezione dei livelli fisico-infrastrutturale e logico-informativo, URSI 2023, pp. 7 ss.

14. V. ampiamente CLUSIT 2024.

15. FERRARESE 2022 si chiede se tali nuovi poteri siano ancora riconducibili alla «“tunica” larga e accogliente» (p. 48) di una governance in cui i poteri sono visibili, richiamando sul punto gli scritti di Norberto Bobbio sulla democrazia come governo del potere visibile.

16. Su tali profili v. LONGO 2024.

17. Il tema è ben presente da almeno un ventennio negli indirizzi politici eurounionali. Cfr. già COM(2001) 298 *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, secondo cui «La sicurezza sta diventando un tema di assoluta priorità perché le comunicazioni e le informazioni sono ormai fattori determinanti dello sviluppo economico e sociale. Le reti e i sistemi di informazione veicolano un volume e una pluralità di servizi e dati ancora inconcepibili fino a pochi anni fa. La loro disponibilità è essenziale per altre infrastrutture quali la rete idrica e la rete elettrica. Poiché tutti, dall'impresa al cittadino privato, alla pubblica amministrazione, desiderano avvalersi delle possibilità offerte dalle reti di comunicazione, la sicurezza di tali sistemi diventa un presupposto essenziale per ulteriori progressi» (p. 6). La comunicazione già riconduceva le misure in materia di sicurezza informatica alle politiche in materia di telecomunicazioni, protezione dei dati e criminalità informatica.

18. In tal senso, ancora FERRARESE 2022, pp. 153 ss.

In questo scenario, tuttavia, l'ancoraggio esclusivo della cybersicurezza alle funzioni di protezione della sicurezza nazionale e la conseguente definizione a livello interno di un reticolo di funzioni e compiti tutti riferibili agli apparati di Governo tradiscono un approccio verticale e tecnicistico, che trascura la sua dimensione plurale¹⁹.

D'altro canto, il quadro regolatorio eurounionale esclude un approdo di tipo securitario, cioè il rafforzamento della cybersicurezza imperniato soltanto su meccanismi reattivi (se non addirittura repressivi e sanzionatori), ma non preclude differenziazioni in fase di adeguamento. Per tale ragione è quantomai opportuna la ricerca di soluzioni regolatorie e attuative il più possibile distanti da modelli di tipo impositivo, rimessi cioè alla mera adozione di nuovi carichi regolatori (oneri e obblighi) specie su soggetti privati (piccole e medie imprese) e amministrazioni pubbliche. Tali considerazioni paiono più ancora necessarie ove si considerino taluni ulteriori profili della cybersicurezza, come la cyberdefence o la cyberintelligence, che spingono verso una sempre maggiore autonomia della funzione mantenendola evidentemente saldamente innestata nella sola azione di Governo²⁰, e talune nuove proposte regolatorie attualmente all'esame del Parlamento.

2.1. I settori interrelati con la funzione di cybersicurezza

Le nuove e più severe misure di cybersicurezza introdotte dalla normativa recente interessano i settori economici più diversi, da quello bancario e finanziario al settore dell'energia, dal settore alimentare a quello dei servizi digitali (infrastrutture, reti, e-commerce, motori di ricerca, cloud ecc.) oltre che le attività delle amministrazioni pubbliche²¹. L'obiettivo principe di tale regolazione resta quello di prevenire e gestire gli attacchi informatici, e su questo aspetto i dati del *Global Cybersecurity Index 2024* collocano l'Italia tra i Paesi più virtuosi²². Si tratta ovviamente di un monitoraggio orientato e condizionato da una visione tecnocentrica, ontologicamente espressa peraltro dall'ITU, la quale non considera altre rilevanti variabili, riferibili alla dimensione plurale di cui si è detto sopra. Manca per esempio una griglia delle competenze e degli interventi diffusi che per via mediata impattano significativamente sul livello complessivo di cybersicurezza²³. Un esame più capillare dei dati relativi agli attacchi informatici andati a buon fine negli ultimi mesi, rivolti ai sistemi IT di amministrazioni pubbliche o imprese di piccole e medie dimensioni, mostra proprio una vulnerabilità complessiva ampia e sfaccettata, certamente di tipo tecnico-strutturale, ma non soltanto. L'efficacia degli

19. Sul rapporto tra tecnica e decisione politica, v. ampiamente CARDONE 2021.

20. Sulla cybersicurezza come funzione amministrativa autonoma, v. le considerazioni di URSI 2023. Sulla ulteriore vercalizzazione dei poteri di sicurezza pubblica v. il ddl AC1236 (Disposizioni in materia di sicurezza pubblica, di tutela del personale in servizio, nonché di vittime dell'usura e di ordinamento penitenziario) di iniziativa del Ministro dell'interno (Governo Meloni-I) già approvato dalla Camera e alla data attuale in commissione in Senato.

21. Ultimo in ordine di tempo è il regolamento (UE) 2024/2847 già citato. Di recente recepimento sono poi le due direttive n. 2022/2555 sulla resilienza dei soggetti critici e n. 2022/2557 (cosiddetta NIS 2) recepite coi decreti legislativi nn. 134 e 138 del 2024. I due decreti sono stati approvati in via definitiva dal Consiglio dei Ministri nella seduta n. 91 del 7 agosto 2024, a seguito dell'esame parlamentare per i pareri concluso il 27 luglio (sull'iter dello schema di decreto legislativo, cfr. XIX leg., Camera dei deputati, Atto del Governo n. 164). Per uno sguardo di sintesi sulla regolazione in materia di cybersicurezza, v. LONGO 2024-A, p. 203 ss. In particolare, sulla direttiva NIS 2, v. CASAROSA-COMANDÈ 2024; BUFFA 2023; BAVETTA 2022; ZORZI GIUSTINIANI 2022, p. 56.

22. Cfr. ITU 2024. Il rapporto si basa sui dati forniti dai punti di contatto nazionali (in Italia l'ACN) ed è poi elaborato secondo un approccio multi-stakeholder. L'Italia rientra tra i Paesi più virtuosi assieme ad altri 45 Stati, ritenuti molto solidi in relazione ai cinque parametri usati per la classificazione (Legal, Technical, Organizational, Capacity Development, Cooperation Measures).

23. In tal senso, v. CLUSIT 2024, in particolare l'*Approfondimento Italia e PA*, che riferisce di un aumento esponenziale del numero di attacchi rivolti alle piccole e piccolissime pubbliche amministrazioni, probabilmente a causa dei ritardi nel percorso di digitalizzazione e formazione del personale in termini di cultura del digitale.

attacchi trova per esempio nel tardivo o parziale processo di digitalizzazione e nell'assenza o nell'inadeguatezza di percorsi formativi sulla sicurezza informatica e sulla gestione del rischio un grande alleato. Resta, dunque, centrale la dimensione ampia e poliedrica della cybersicurezza, per il cui rafforzamento sono determinanti l'azione socio-educativa sul territorio, il supporto amministrativo locale alle piccole e piccolissime imprese, le azioni di monitoraggio e partecipazione sui territori.

Se cioè la cybersicurezza deve essere un'agonista della transizione digitale, è bene che nella sua governance vengano innestati adeguati contrappesi e che si attivino altre competenze, nella misura in cui esse risultino tanto legittime quanto necessarie²⁴. Si pensi per esempio ai settori liminari alla dimensione dell'"ordine pubblico e della sicurezza", cioè a quei settori confinanti con tale materia che spetta in via esclusiva al legislatore statale, ma che per l'appunto non esclude interventi regionali²⁵. L'intervento dello Stato cioè in "materia" di sicurezza non escluderebbe interventi regionali

in settori confinanti, meno a rischio di erosione rispetto ad esempio ai casi di materie trasversali come il coordinamento informatico che di fatto attraversano, attraendone parti, spazi limitrofi di competenza regionale²⁶. Accanto alla "sicurezza in 'senso stretto' (o *sicurezza primaria*)"²⁷ che spetta allo Stato esistono ambiti di "sicurezza secondaria (o *sicurezza in senso lato*)"²⁸, che ricomprende «un fascio di funzioni intrecciate, corrispondenti a plurime e diversificate competenze di spettanza anche regionale»²⁹ e che risponde a quell'esigenza di coordinamento tra Stato e Regioni che la legge statale può disciplinare anche nella materia dell'ordine pubblico e sicurezza (*ex art. 118, terzo comma, Cost.*). Con riguardo all'ambito della digitalizzazione e alla sicurezza delle persone nello spazio digitale si può qui menzionare il caso del contrasto al cyberbullismo³⁰, che richiede interventi non soltanto di tipo penale o di polizia, ma anche e soprattutto di carattere educativo e social-preventivo³¹. Non sono neppure mancate talune sperimentazioni linguistico/normative, come quella

24. Evidenzia i limiti delle attuali forme di controllo parlamentare sulle attività di cybersicurezza facenti capo alla Presidenza del Consiglio e all'Agenzia per la Cybersicurezza GIUPPONI 2024, specie p. 297. Più in generale, con uno sguardo filosofico e pragmatico assieme, sui modelli di governance del digitale, interessanti le osservazioni di BENANTI 2022, specie le pp. 133 ss., che prospetta una governance delle intelligenze artificiali inclusiva, in cui si annodano aspetti tecnici ed etici, la quale dovrebbe intercettare tutta la comunità di riferimento per definire assetti organizzativi e regole possibili (i migliori possibili).

25. Corte cost. sentenza n. 226 del 2010, Diritto 5.2, che richiama *ex plurimis* le sentenze n. 129 del 2009; n. 237 e n. 222 del 2006; n. 383 e n. 95 del 2005; n. 428 del 2004.

26. Cfr. Corte cost. n. 285 del 2019, Diritto 2.3, in cui si legge «Per costante orientamento di questa Corte, allora, l'endiadi "ordine pubblico e sicurezza", di cui all'art. 117, secondo comma, lettera h), Cost., allude a una materia in senso proprio, e cioè a una materia oggettivamente delimitata che di per sé non esclude l'intervento regionale in settori ad essa liminari».

27. *Ibidem*.

28. *Ibidem*.

29. *Ibidem*.

30. In tal senso, v. la l.r. Regione Umbria 9 maggio 2018, n. 4 (*Disciplina degli interventi regionali per la prevenzione e il contrasto del fenomeno del bullismo e del cyberbullismo – Modificazioni a leggi regionali*), che ha superato il vaglio della Corte Costituzionale, secondo cui la Regione si è legittimamente mossa nell'ambito della propria competenza di promozione culturale e politica socio-assistenziale, senza "tracimare" in quella statale della tutela dell'ordine pubblico e della sicurezza: «Il legislatore regionale è piuttosto intervenuto in un'ottica di prevenzione del bullismo quale problema di interesse sociale generale, per tutelare e valorizzare la crescita educativa, sociale e psicologica dei minorenni, perseguendo finalità di prevenzione, estranee alla materia della tutela dell'ordine pubblico e della sicurezza.» (Corte cost. n. 116 del 2019, Diritto 3.4.)

31. Sul modello securitario nell'approccio del legislatore statale, v. ampiamente le riflessioni a prima lettura sulla legge n. 90/2024 contenute nei saggi apparsi in FIORINELLI-GIANNELLI 2024.

relativa al “sistema integrato e unitario di sicurezza nazionale”³², che vuole alludere alla pluralità degli interventi di soggetti diversi ciascuno nell’ambito delle proprie competenze e responsabilità. Si tratta di un terreno già arato, nel solco del quale potrebbe avviarsi forse una riflessione anche per i profili di nostro interesse. Per quanto, anche tale modello – come evidenziato nella letteratura più avveduta sulla materia – parrebbe confermare un’impronta securitaria di tipo verticale³³.

Nel quadro sopra delineato, si consideri poi che per numerosità e ampiezza di compiti un ruolo di assoluto protagonismo spetta all’Agenzia per la Cybersicurezza Nazionale (ACN). Pur se di recente istituzione (2021), molte e approfondite risultano già le riflessioni sulla sua natura giuridica, e specialmente su compiti e funzioni ad essa assegnati³⁴. Senza qui entrare nel dettaglio di un reticolo

regolativo che s’infittisce al pari dell’aumento delle minacce cyber, occorre qui almeno segnalare che parimenti cresce il numero di compiti affidati alla nostra agenzia³⁵.

In tale direzione vanno per esempio le proposte contenute nel disegno di legge d’iniziativa governativa AS1146 in materia di intelligenza artificiale, attualmente all’esame del Senato come collegato alla legge di bilancio³⁶.

Tale progetto, infatti, assegna all’ACN ulteriori nuovi compiti, tra cui quello di promuovere e sviluppare ogni iniziativa, anche di partenariato pubblico-privato, finalizzata a valorizzare l’intelligenza artificiale come risorsa per il rafforzamento della cybersicurezza nazionale, concentrando in essa poteri che pure potevano convergere su altre autorità³⁷. Se il disegno di legge verrà adottato nel testo attualmente in discussione, dunque, all’ACN,

32. La formula è tratta dall’art. 1, co. 2, del d.l. 20 febbraio 2017, n. 14 (*Disposizioni urgenti in materia di sicurezza delle città*), conv. con modifiche nella legge n. 48/2017: «Ai fini del presente decreto, si intende per sicurezza integrata l’insieme degli interventi assicurati dallo Stato, dalle Regioni, dalle Province autonome di Trento e Bolzano e dagli enti locali, nonché da altri soggetti istituzionali, al fine di concorrere, ciascuno nell’ambito delle proprie competenze e responsabilità, alla promozione e all’attuazione di un sistema unitario e integrato di sicurezza per il benessere delle comunità territoriali.» Il “benessere delle comunità territoriali” giustificerebbe quindi la previsione legislativa di forme di coordinamento tra Stato e Regioni, e la promozione della sicurezza integrata deve tener conto «(...) della necessità di migliorare la qualità della vita e del territorio e di favorire l’inclusione sociale e la riqualificazione socio-culturale delle aree interessate» (art. 2, co. 1-bis). Secondo FAMILIETTI 2020, si tratterebbe però di una definizione «più che volta a delimitare l’ambito contenutistico degli interventi, ad individuare i soggetti protagonisti della “sicurezza integrata” e gli strumenti volti al perseguimento degli obiettivi» (p. 177).

33. Sulla persistenza di una impronta verticale. v. ANTONELLI 2017; NOBILI 2018, p. 61 ss.

34. Tra gli altri, v. GIUPPONI 2024; RICOTTA 2023, p. 97 ss.; GOLISANO 2022; FORGIONE 2022; SOLA 2022; CONTALDO 2023; POLETTI 2023; volendo, PIETRANGELO 2024; GIANNELLI 2024.

35. Cfr. al proposito il DPCM 15 giugno 2022 e il DPCM 1° settembre 2022, mediante cui sono state trasferite in capo all’Agenzia per la Cybersicurezza Nazionale le funzioni in materia di cybersicurezza precedentemente assegnate al Ministero dello Sviluppo Economico (MISE), all’Agenzia per l’Italia digitale (AgID) e al Dipartimento per la trasformazione digitale della PCM.

36. XIX leg., AS 1146 (Disposizioni e delega al Governo in materia di intelligenza artificiale), d’iniziativa del Presidente del Consiglio e del Ministro della giustizia (Governo Meloni-I). Il ddl è attualmente all’esame in sede referente presso le Commissioni riunite 8^a (Ambiente, transizione ecologica, energia, lavori pubblici, comunicazioni, innovazione tecnologica) e 10^a (Affari sociali, sanità, lavoro pubblico e privato, previdenza sociale).

37. Cfr. l’art. 16 del ddl, che modifica l’art. 7, comma 1, del d.l. 14 giugno 2021, n. 82 istitutivo dell’Agenzia. Sulla cybersicurezza come condizione per lo sviluppo di sistemi basati sull’intelligenza artificiale, quantomai efficace il testo del Considerando 76 del Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull’intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull’intelligenza artificiale): la «cibersicurezza svolge un ruolo cruciale nel garantire che i sistemi di IA siano resilienti ai tentativi compiuti da terzi con intenzioni malevole

andranno ulteriori compiti di carattere ispettivo e sanzionatorio, e all'Agenzia per l'Italia digitale – altra agenzia governativa che opera nel settore della digitalizzazione – spetterebbe il controllo sullo sviluppo dell'IA negli enti pubblici e la definizione delle misure di certificazione e accreditamento degli sviluppatori³⁸.

3. Per concludere, con alcuni interrogativi

La scelta di un modello di governo della cybersicurezza tendenzialmente accentrato è confermato nei documenti di indirizzo che delineano la strategia nazionale in materia³⁹, per quanto le misure in essi previste cerchino di enfatizzare anche le azioni di coordinamento degli interventi di tutti i soggetti pubblici e privati coinvolti. In definitiva, siamo di

fronte a questioni inedite – almeno nei termini che la cybersicurezza sta assumendo da ultimo – che impattano sul difficile equilibrio tra esigenze di sicurezza pubblica e di protezione delle libertà fondamentali, ma aprono al contempo a nuovi interrogativi⁴⁰.

Le tecniche di sicurezza informatica evolvono, per rispondere alla specializzazione e all'aumento per numero e superficie di attacco delle aggressioni, e i requisiti di sicurezza delle reti e dei sistemi di informazione si irrobustiscono in una dinamica di azione e reazione tra tecniche di hacking e di anti-hacking⁴¹. In questo scenario, il ruolo delle autorità pubbliche è decisivo, a patto che esse non rinuncino a valorizzare le azioni coordinate e

che, sfruttando le vulnerabilità del sistema, mirano ad alterarne l'uso, il comportamento, le prestazioni o a comprometterne le proprietà di sicurezza.».

38. Dal 1993 ad oggi la “materia della digitalizzazione” è stata affidata sempre ad agenzie governative, pur con rilevanti differenze sotto il profilo organizzativo e funzionale. Dal 1993, quando fu costituita la prima Autorità per l'informatica nella pubblica amministrazione (AIPA), passando per il Centro tecnico per la Rupa (1997), il Cnipa (2003), l'Agenzia per la diffusione delle tecnologie per l'innovazione (2006), il DigitPA (2009) fino all'Agenzia Italia digitale (2012) e all'ACN.

39. La *Strategia nazionale di Cybersicurezza 2022-2026* (adottata nel maggio 2022) e il relativo Piano di implementazione, previsto dall'art. 2 co. 1, lett. b) del d.l. n. 82/2021, convertito nella legge n.109/2021 (istitutivo della Agenzia per la Cybersicurezza Nazionale - ACN), dispongono il raggiungimento di 82 nuove misure entro il 2026. Molteplici gli obiettivi: proteggere asset strategici nazionali attraverso un approccio risk based, adottando un “quadro normativo efficiente per una transizione digitale resiliente del Paese”; rispondere alle minacce e crisi cyber nazionali attraverso sistemi di monitoraggio, rilevamento, analisi e processi di sicurezza; sviluppare tecnologie digitali sicure attraverso strumenti e iniziative che supportino attività di ricerca, centri di eccellenza e imprese del settore.

40. Si pensi per esempio alla cosiddetta “direttiva Monti” (d.P.C.M. 24 gennaio 2013, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*) che imponeva a carico di alcuni operatori privati (es. i fornitori di servizi di comunicazione elettronica e reti pubbliche di comunicazione; i gestori di infrastrutture critiche di rilievo nazionale ed europeo) nuovi obblighi informativi a favore del Nucleo per la sicurezza cibernetica. Questi soggetti dovevano comunicare le violazioni “significative” della sicurezza o dell'integrità dei propri sistemi informatici, fornendo informazioni e dati (e quindi consentendo l'accesso a basi di dati nelle quali sono raccolti e trattati dati personali). E già al tempo le “esigenze di adempimento delle funzioni istituzionali” (di cybersicurezza) che le norme in materia di segreto e sicurezza nazionale pongono alla base di questo accesso a dati personali e sensibili in possesso di soggetti privati non parevano garanzia sufficiente per la tutela dei diritti fondamentali coinvolti. Sul punto v. ampiamente RESTA 2024.

41. Il rischio inteso come potenziale perdita o perturbazione causata da un incidente deve essere valutato sulla base dell'entità della perdita o perturbazione e della probabilità che l'incidente si verifichi; questo rischio diventa poi “significativo” se ha delle caratteristiche tecniche per cui si può presumere una “probabilità elevata” di provocare un incidente con un impatto negativo grave. Così le definizioni di “rischio di cybersicurezza” (art. 1, co. 1, n. 37) e “rischio di cybersicurezza significativo” (art. 1, co. 1, n. 38) nel regolamento (UE) 2024/2847 (regolamento sulla cyberresilienza).

collettive, pilastro della sicurezza digitale, e non si limitino "solo" a normarla⁴².

Si tratta in definitiva di aggiungere un tassello alla riflessione sulle "vulnerabilità" dell'attuale governance del digitale, a partire dall'osservazione delle dinamiche di governo di un settore solo

all'apparenza fortemente tecnico; e di considerare nuove domande, interrogandosi anzitutto su quale sia oggi *effettivamente* la pluralità di interessi che l'esercizio della funzione pubblica di cybersicurezza mira a tutelare.

Riferimenti bibliografici

- L. ABBA, A. LAZZARONI, M. PIETRANGELO (a cura di) (2022), *La Internet governance e le sfide della trasformazione digitale*, Editoriale Scientifica, 2022
- V. ANTONELLI (2017), *La sicurezza in città ovvero l'iperbole della sicurezza urbana*, in "Istituzioni del federalismo", 2017, n. 1
- R. BALDONI (2024), *Charting Digital Sovereignty: A Survival Playbook. How to assess and to improve the level of digital sovereignty of a country*, independently published, 2024
- F. BAVETTA (2022), *Direttiva NIS 2: verso un innalzamento dei livelli di cybersicurezza a livello europeo*, in "MediaLaws", 2022, n. 3
- P. BENANTI (2022), *Human in the loop. Decisioni umane e intelligenze artificiali*, Mondadori, 2022
- M. BETZU (2021), *I poteri privati nella società digitale: oligopoli e antitrust*, in "Diritto pubblico", 2021, n. 3
- A. BRADFORD (2023), *Digital Empires. The Global Battle to Regulate Technology*, Oxford University Press, 2023
- M. BUFFA (2023), *La direttiva NIS II cybersecurity in Europa: tra innovazione, formazione e diritto vivente*, in "Democrazia e Diritti Sociali", 2023, n. 1
- A. CARDONE (2021), *"Decisione algoritmica" vs decisione politica? A.I., Legge, Democrazia*, Editoriale Scientifica, 2021
- G. CERRINA FERONI, C. FONTANA, E.C. RAFFIOTTA (a cura di) (2022), *AI Anthology. Profili giuridici, economici e sociali dell'intelligenza artificiale*, il Mulino, 2022
- CLUSIT (2024), *Rapporto 2024 sulla sicurezza ICT in Italia*, ottobre 2024
- F. CASAROSA, G. COMANDÈ (2024), *Aspettando la NIS2: ovvero il diritto privato della cybersecurity*, in "Il Diritto dell'informazione e dell'informatica", 2024, n. 1
- A. CONTALDO (2023), *L'attuazione della "cybersecurity" nazionale: un difficile esercizio di una funzione pubblica*, in "Lo Stato", 2023, n. 21
- G. FAMIGLIETTI (2020), *Il patrocinio legale a spese della Regione nel quadro del "magnetismo securitario" (a partire da Corte cost. n. 285 del 2019)*, in "Forum di Quaderni Costituzionali", 2020, n. 2
- M.R. FERRARESE (2022), *Poteri nuovi. Privati, penetranti, opachi*, il Mulino, 2022

42. Sulla rilevanza delle azioni collettive nel settore della cybersicurezza insiste particolarmente il National Cyber Security Center inglese (cfr. NCSC *Annual Review* cit.). Sui carichi regolatori, da ultimo v. EUROPEAN COMMISSION, *The future of European competitiveness*, September 2024 (cosiddetto "Rapporti Draghi"), secondo cui sono oltre 350 gli atti normativi dell'Unione che regolano l'utilizzo delle tecnologie digitali. Tali atti gravano con oneri e obblighi specie sulle start-up che operano nei settori più innovativi. Uno stock normativo reso ancor più pesante dalla sistematica violazione da parte degli Stati membri del divieto di gold plating (cioè di superare in fase di recepimento o attuazione le misure standard contenute negli atti dell'Unione).

- G. FINOCCHIARIO, L. BALESTRA, M. TIMOTEO (a cura di) (2022), *Major Legal Trends in the Digital Economy. The Approach of the EU, the US, and China*, il Mulino, 2022
- G. FIORINELLI, M. GIANNELLI (a cura di) (2024), *Il DDL Cybersicurezza (AC 1717). Problemi e prospettive in vista del recepimento della NIS 2*, sezione monografica, in “Rivista italiana di informatica e diritto”, 2024, n. 1
- I. FORGIONE (2022), *Il ruolo strategico dell’agenzia nazionale per la cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna*, in “Diritto amministrativo”, 2022, n. 4
- M. GIANNELLI (2024), *Il contributo dei livelli di governo substatali al raggiungimento degli obiettivi del ddl Cybersicurezza*, in “Rivista italiana di informatica e diritto”, 2024, n. 1
- L. GOLISANO (2022), *Il governo del digitale: strutture di governo e innovazione digitale*, in “Giornale di diritto amministrativo”, 2022, n. 6
- T.F. GIUPPONI (2024), *Il governo nazionale della cybersicurezza*, in “Quaderni costituzionali”, 2024, n. 2
- ITU (2024), *Global Cybersecurity Index 2024*, 5th edition, 2024
- R. LAKSHMANAN (2024), *Russian RomCom Attacks Target Ukrainian Government with New SingleCamper RAT Variant*, in “The Hacker News”, October 17, 2024
- E. LONGO (2024), *Il diritto costituzionale e la cybersicurezza. Analisi di un volto nuovo del potere*, in “Rassegna parlamentare”, 2024, n. 2
- E. LONGO (2024-A), *La disciplina della cybersecurity nell’Unione europea e in Italia*, in S. Calzolaio, A. Iannuzzi, E. Longo et al., “La regolazione europea della società digitale”, Giappichelli, 2024
- C. MOSCA (2021), *La sicurezza: valori, modelli e prassi istituzionali*, Editoriale Scientifica, 2021
- G.G. NOBILI (2018), *Le linee generali delle politiche pubbliche per la promozione della sicurezza integrata e la sicurezza urbana nel coordinamento tra Stato e Regioni*, in G.G. Nobili, T.F. Giupponi, E. Ricifari, N. Gallo (a cura di), “La sicurezza delle città. La sicurezza urbana e integrata”, Franco Angeli, 2018
- M. PIETRANGELO (2024), *Per un modello nazionale di cybersicurezza cooperativa e resilienza collaborativa*, in “Rivista italiana di informatica e diritto”, 2024, n. 1
- S. POLETTI (2023), *La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica*, in “MediaLaws”, 2023, n. 2
- O. POLLICINO (2023), *Potere digitale*, in “Potere e Costituzione”, Enciclopedia del diritto, I Tematici, vol. 5, Giuffrè, 2023
- F. RESTA (2024), *Cybersicurezza e protezione dati: un rapporto ambivalente*, in “Rivista italiana di informatica e diritto”, 2024, n. 2
- G. RESTA (2023), *Poteri privati e regolazione*, in “Potere e Costituzione”, Enciclopedia del diritto, I Tematici, vol. 5, Giuffrè, 2023
- F.N. RICOTTA (2023), *Agenzia per la “cybersicurezza” nazionale, sicurezza della Repubblica e investigazioni dell’Autorità giudiziaria*, in “Diritto penale contemporaneo”, 2023, n. 1
- M.A. RIZZI, F. SERINI (2024), *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*, in “Rivista italiana di informatica e diritto”, 2024, n. 2
- A. SIMONCINI (2022), *La dimensione costituzionale dell’intelligenza artificiale*, in G. Cerrina Feroni, C. Fontana, E.C. Raffiotta (a cura di), “AI Anthology. Profili giuridici, economici e sociali dell’intelligenza artificiale”, il Mulino, 2022

- A. SOLA (2022), *Economie dei dati, nuovi poteri ed autorità amministrative: il caso dell'Agenzia per la cybersicurezza nazionale*, in "MediaLaws", 2022, n. 3
- F. SORO (2019), *Regolazione e governance del mondo digitale. Profili del diritto della rete in USA, UE e Italia*, Giappichelli, 2019
- S. STAIANO (2024), *Nel margine del caos. Trasformazione e conservazione dell'ordinamento costituzionale*, in "Rivista AIC", 2024, n. 11
- L. TORCHIA (2024), *Poteri pubblici e poteri privati nel mondo digitale*, in "il Mulino", 2024, n. 1
- R. URSI (a cura di) (2023), *La sicurezza cibernetica come funzione pubblica*, in Id. (a cura di), "La sicurezza nel cyberspazio", Franco Angeli, 2023
- R. URSI (2022), *La sicurezza pubblica*, il Mulino, 2022
- A. VEDDER (2019), *Safety, Security and Ethics*, in A. Vedder, J. Schroers, C. Ducuing, P. Valcke (eds.), "Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security", Intersentia, 2019
- G. ZACCARIA (2022), *Postdiritto. Nuove fonti, nuove categorie*, il Mulino, 2022
- F. ZORZI GIUSTINIANI (2022), *La nuova direttiva europea per la cybersicurezza e un ulteriore ampliamento del diritto all'oblio digitale*, in "Nomos", 2022, n. 3



STEFANO PIETROPAOLI

Dalla sorveglianza al controllo: la parabola della governamentalità algoritmica

Il presente lavoro esplora l'evoluzione del potere nella società contemporanea, analizzando la transizione dalla sorveglianza alla governamentalità algoritmica. L'autore discute come la rivoluzione digitale abbia trasformato ogni aspetto della vita umana in dati, dando origine a nuove forme di controllo sociale. Queste forme di controllo, basate su algoritmi e big data, sfidano le tradizionali nozioni di libertà, diritti e democrazia. Vengono esaminate le implicazioni di questo nuovo paradigma, inclusi i rischi di discriminazione algoritmica e la perdita di autonomia individuale. Infine, si considerano le possibilità di resistenza a questo potere diffuso e invisibile, proponendo nuove forme di soggettività e di lotta.

Governamentalità algoritmica – Sorveglianza – Controllo sociale – Discriminazione algoritmica – Resistenza

From surveillance to control: the evolution of algorithmic governmentality

This paper explores the evolution of power in contemporary society, analyzing the transition from surveillance to algorithmic governmentality. The author discusses how the digital revolution has transformed every aspect of human life into data, giving rise to new forms of social control. These forms of control, based on algorithms and big data, challenge traditional notions of freedom, rights, and democracy. The implications of this new paradigm, including the risks of algorithmic discrimination and the loss of individual autonomy, are examined. Finally, the possibilities of resistance to this diffuse and invisible power are considered, proposing new forms of subjectivity and struggle.

Algorithmic governmentality – Surveillance – Social control – Algorithmic discrimination – Resistance

L'Autore è professore associato di Filosofia del diritto presso l'Università degli Studi di Firenze

Questo contributo fa parte della sezione monografica *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà*, a cura di Marina Pietrangelo

SOMMARIO: Premessa. – Oltre la società disciplinare. – La governamentalità algoritmica. – Resistere alla società del controllo?

Premessa

La rivoluzione digitale sembra aver ormai coinvolto ogni aspetto della vita umana. Tutto sembra misurabile, quantificabile, “datificabile”: ogni azione, ogni esperienza, ogni secondo della nostra esistenza sono trasformati in dati affinché possano essere elaborati – “manipolati” – dalle macchine.

Questa straordinaria massa di informazioni, unita alla crescente potenza di calcolo e agli avanzamenti nell’intelligenza artificiale, ha dato vita a nuove forme di potere. Si stanno così ridefinendo i meccanismi di governo dei popoli e gli equilibri tra Stati, mercato e cittadini. Il potere si manifesta in modo sempre più sottile e pervasivo attraverso strumenti di analisi predittiva e meccanismi di condizionamento dei comportamenti individuali. Questo nuovo paradigma è compendiato dal concetto di “governamentalità algoritmica”, elaborato da studiosi come Antoinette Rouvroy e Bernard Stiegler.

Basata sulla raccolta sistematica di dati e sulla loro elaborazione attraverso algoritmi complessi, questa nuova governamentalità presenta caratteristiche diverse rispetto all’idea originariamente proposta da Michel Foucault. Non si tratta più di strumenti diretti a “sorvegliare e punire”: attraverso l’analisi dei dati e l’individuazione di *pattern* e correlazioni, il nuovo modello promette di anticipare e prevenire i comportamenti indesiderati: la previsione consente di intervenire preventivamente. Inoltre, la governamentalità algoritmica sfugge alla distinzione otto-novecentesca tra pubblico e privato. Le grandi aziende tecnologiche diventano

attori sempre più rilevanti nella gestione sociale, affiancandosi alle istituzioni pubbliche o, come accade sempre più spesso, sostituendosi *in toto* a queste. E ciò avviene attraverso meccanismi di controllo algoritmico del tutto opachi. A differenza dei sistemi tradizionali di sorveglianza, comprensibili o almeno visibili, gli algoritmi sono imperscrutabili, sia per la loro complessità tecnica sia per la segretezza commerciale che li contraddistingue. Questa assenza di trasparenza rende estremamente difficile contestare le decisioni e resistere alle forme di ingiustizia generate da questi sistemi.

La rivoluzione digitale sembra offrire enormi potenzialità in termini di efficienza, precisione e personalizzazione. Ma sull’altare di questo presunto progresso vengono sacrificati i successi faticosamente raggiunti durante “l’età dei diritti”: non soltanto si consolidano e amplificano disuguaglianze già esistenti, ma si creano nuove forme di discriminazione e di esclusione sociale.

Oltre la società disciplinare

Michel Foucault, nel suo celebre *Sorvegliare e punire* del 1975¹, ha delineato il passaggio tra XVIII e XIX secolo da una società basata sul potere sovrano – caratterizzato da punizioni pubbliche e spettacolari – a una società disciplinare, in cui il potere si esercita attraverso istituzioni di confinamento come scuole, fabbriche, ospedali e prigioni, che modellano i corpi e le menti degli individui attraverso la sorveglianza costante e la normalizzazione dei comportamenti.

Com’è noto, il modello paradigmatico di questa forma di potere è il *panopticon* ideato da Jeremy

1. FOUCAULT 2019.

Bentham²: una struttura architettonica³ che permette di osservare costantemente i detenuti senza che questi sappiano di essere osservati, inducendoli così all'autocontrollo. Dalla torre centrale una guardia può osservare tutti i prigionieri, disposti in celle che circondano la struttura principale. I prigionieri non possono sapere quando sono osservati, e pertanto "internalizzano" la sorveglianza, disciplinando se stessi. Questa incertezza, infatti, induce un comportamento disciplinato, senza bisogno di una costante presenza fisica dell'autorità. È un potere visibile ma inverificabile.

Questo meccanismo, secondo Foucault, è stato applicato con sempre maggiore efficacia non soltanto alle prigioni⁴, ma anche alle scuole, agli ospedali, alle caserme, alle fabbriche, e in definitiva a tutti quegli spazi delimitati e istituzionali capaci di concentrare, suddividere, ordinare e comporre forze produttive superiori alla somma delle parti.

A partire dal 1978⁵ Michel Foucault approfondisce la sua analisi del potere e delle tecniche di governo, introducendo il concetto di "governamentalità", che diventa l'anno successivo oggetto centrale delle lezioni – raccolte poi sotto il titolo *Nascita della biopolitica*⁶ – da lui dedicate alle trasformazioni del governo dalla sovranità classica alla biopolitica moderna.

Con questa espressione Foucault si riferisce a un insieme di pratiche e tecniche attraverso le quali il potere viene esercitato non solo a livello statale, ma anche in una vasta gamma di contesti sociali, economici e personali. Il potere si impiega dunque non soltanto attraverso istituzioni tradizionali (come le leggi e le politiche statali), ma anche attraverso una serie di pratiche che regolano il comportamento e la mentalità delle persone⁷. Si tratta dunque dell'esercizio non soltanto di un controllo diretto, ma anche della capacità del potere di

influenzare indirettamente le scelte, i desideri e le credenze delle persone.

La governamentalità secondo Foucault ha contribuito allo sviluppo dello Stato moderno, con le sue burocrazie, istituzioni e pratiche amministrative. Tuttavia, questo modello disciplinare ha espresso tutto il suo potenziale in un arco di tempo limitato: dalla fine delle società di sovranità (caratterizzate dal potere di decidere sulla vita e sulla morte) alla Seconda Guerra Mondiale. Come presagito a livello letterario nel 1961 da William Burroughs⁸, nuove forme di controllo – emerse con lo sviluppo tecnologico di metà Novecento (come la tecnologia farmaceutica, quella nucleare e quella genetica) – stavano rendendo obsolete le istituzioni disciplinari, segnando così l'inevitabile transizione verso forme di controllo più precise e veloci.

Sul piano teorico (nonostante alcune precedenti intuizioni di Paul Virilio⁹), è stato Gilles Deleuze nel 1990 a cogliere il senso profondo della sostituzione del modello disciplinare con una nuova configurazione del potere¹⁰: la società della sorveglianza ha iniziato a trasformarsi in una "società del controllo", in cui le rigide strutture di confinamento otto-novecentesche hanno iniziato a rarefarsi, in favore di forme di controllo più flessibili, fluide, continue e pervasive. Questo slittamento è esemplificato dalla transizione dal lavoro di fabbrica al telelavoro, o dall'educazione confinata nelle aule scolastiche alla formazione permanente. La sorveglianza esercitata in spazi chiusi diventa controllo: fluido, modulabile, estensibile a tutti gli ambiti della vita.

La transizione verso questa nuova forma del potere, per Deleuze, è stata resa possibile dalle tecnologie digitali. Dopo le macchine semplici delle società di sovranità e le macchine energetiche delle società disciplinari, giunge il tempo delle

2. BENTHAM 1791/2009.

3. LA MONICA 2014.

4. SBRICCOLI 1977.

5. FOUCAULT 2005-B.

6. FOUCAULT 2005-A.

7. Sul tema la letteratura è sterminata; segnalo qui almeno: BAZZICALUPO 2013; BAZZICALUPO 2016; CHIGNOLA 2011, CHIGNOLA 2014-A; CHIGNOLA 2014-B; CHIGNOLA 2022; LUCE 2009; MEZZADRA 2008.

8. BURROUGHS 2003.

9. VIRILIO 1977.

10. DELEUZE 2012.

macchine informatiche e dei computer. Invece di essere confinati in spazi delimitati (come la scuola, la fabbrica, la prigione), gli individui si trovano adesso in un flusso costante e ubiquitario di controllo, immersi in uno spazio i cui confini non sono fisici ma digitali e informatici (quello che oggi chiameremmo *cyberspace*).

Le masse si trasformano in dati e mercati, mentre gli individui diventano “dividuali”. Contro l’idea moderna di un individuo come soggetto stabile, singolare, autonomo e coerente, il dividuale si staglia come un insieme di parti o frammenti che si formano e si riformano continuamente in relazione a contesti sociali, culturali e tecnologici. Le tecnologie digitali frammentano e ricompongono continuamente ciò che siamo, rendendo i soggetti – in quanto ridotti a “dati” – gestibili e manipolabili.

Reti informatiche, big data e algoritmi consentono al potere di adattarsi e modulare costantemente le proprie risposte sulla base dei dati raccolti. Non conta più tanto il sorvegliare per punire, quanto il controllare per condizionare. La sanzione è sempre possibile, certo, ma il potere adesso consegue i suoi obiettivi primariamente grazie alla capacità di indurre nei consociati determinati comportamenti: suggerimenti personalizzati, pubblicità mirata, e variazioni nei prezzi dei servizi basate sull’analisi comportamentale sono tutti strumenti che funzionano in maniera più efficiente del carcere e delle altre istituzioni totali¹¹.

La governamentalità algoritmica

Il controllo sociale si sta avvalendo sempre più dell’uso di tecnologie avanzate, come braccialetti elettronici e altri dispositivi digitali che monitorano e regolano l’accesso e i movimenti delle persone. Questi sistemi operano attraverso una sorveglianza continua e diffusa, superando i tradizionali luoghi di reclusione fisica come prigioni, scuole e ospedali. Le istituzioni tradizionali si stanno adattando a queste nuove dinamiche, trattando gli individui come insiemi di dati da monitorare e gestire.

Questo nuovo modo di esercitare il potere, basato su algoritmi e analisi dei dati, è stato

chiamato da Antoinette Rouvroy “governamentalità algoritmica”¹². A differenza delle forme tradizionali di potere – basate su norme e decisioni umane – la governamentalità algoritmica funziona attraverso meccanismi automatizzati che analizzano grandi quantità di dati in tempo reale. Questo tipo di potere non richiede l’interiorizzazione della sorveglianza (come nel *panopticon* descritto da Foucault), ma funziona principalmente attraverso due strumenti: la profilazione e la (cosiddetta) predizione.

L’ubiquità della raccolta di dati rappresenta il fondamento di questo sistema: ogni nostra interazione digitale, dalle ricerche online agli acquisti, dalle comunicazioni sui social media ai movimenti fisici tracciati dai nostri smartphone, genera una mole impressionante di informazioni. La raccolta costante e pervasiva crea un flusso continuo di dati che alimenta gli algoritmi di analisi e decisione. Gli algoritmi analizzano i nostri dati per creare profili dettagliati delle nostre preferenze, abitudini e comportamenti, permettendo una customizzazione senza precedenti di contenuti, pubblicità e servizi.

Questa personalizzazione, che secondo il mantra delle big tech può “migliorare l’esperienza dell’utente”, rivela prima di tutto che il cittadino moderno è oramai degradato al rango di *user*¹³. Rouvroy sottolinea che la governamentalità algoritmica opera in modo post-individuale, ovvero considera gli individui non come soggetti unici con una propria volontà, ma come insiemi di dati. Ciò conduce a un’assenza di soggettività: un vuoto in cui le persone vengono trattate come mere variabili statistiche. Per riprendere l’immagine proposta da Byung-Chul Han¹⁴, gli individui agiscono come particelle di uno sciame, senza una direzione centrale o un’identità stabile, conformandosi alle opinioni della massa, guidate dal desiderio di approvazione e di *like* piuttosto che da una riflessione autonoma. Tanto veloce quanto superficiale, la comunicazione è meno razionale e più emozionale, ma soprattutto è frammentata e impedisce la formazione di pensieri profondi e duraturi, celebrando una cultura dell’effimero in cui le idee e le relazioni mancano di solidità e continuità.

11. Per un inquadramento del tema, cfr. GOFFMAN 2010.

12. ROUVROY 2008.

13. Mi permetto di rinviare sul tema a PIETROPAOLI 2021.

14. HAN 2016.

In secondo luogo, la personalizzazione rischia di creare “bolle di filtraggio” che limitano la nostra esposizione a idee e informazioni diverse dalle nostre, minando il dibattito pubblico e la formazione di un consenso consapevole¹⁵. Le *filter bubbles*, infatti, isolano gli individui in bolle informative che restringono il campo delle notizie a cui l'individuo è esposto, creando una visione parziale e distorta della realtà. L'isolamento delle idee non solo rafforza le divisioni sociali, ma ostacola anche la possibilità di una comprensione reciproca. In questo modo, le bolle confermano le opinioni e i pregiudizi preesistenti. Questo rinforzo delle convinzioni personali riduce la capacità di confronto e dialogo con idee diverse, col risultato non soltanto di favorire un pensiero conformista e superficiale, ma anche di frammentare il sapere e impoverire la capacità critica.

Ma gli algoritmi non analizzano enormi quantità di dati soltanto per creare profili dettagliati degli individui: la profilazione è finalizzata a “predire” i loro possibili comportamenti futuri. Questo approccio preventivo si estende a vari ambiti: dalla sicurezza pubblica (con sistemi di polizia predittiva) al marketing (con la previsione dei comportamenti di acquisto), fino alla salute (con l'identificazione precoce di potenziali patologie). Solo per fare riferimento a un caso estremamente diffuso: pensiamo ai suggerimenti di acquisto su una piattaforma di *e-commerce*. Gli algoritmi creano un profilo basato sulle preferenze dell'utente, sugli acquisti precedenti e su quelli di utenti considerati simili, e dopo di ciò “predicono” che cosa l'utente potrebbe voler comprare in futuro. Ovviamente, non si tratta di predizione in senso proprio, ma si tratta invece di un condizionamento: la generazione di falsi bisogni o appetiti che vengono indotti grazie a inferenze statistiche.

Mentre Deleuze immaginava nuove forme di controllo continuo e modulare e meccanismi di potere più fluidi, Rouvroy sottolinea che gli algoritmi e i big data rendono oggi possibile un controllo sostanzialmente invisibile eppure onnipresente. Il controllo non si esercita più attraverso la minaccia della punizione o la promessa della ricompensa, ma tramite la previsione e la modulazione sottile dei comportamenti. Mentre nella società

disciplinare il potere era principalmente negativo e repressivo, nella società del controllo esso, infatti, assume una forma più produttiva e “seduttiva”, che sostituisce divieti e punizioni con desideri indotti e condizionamenti.

Se il modello del *panopticon* di Bentham rappresentava la sorveglianza disciplinare, la governamentalità algoritmica opera piuttosto secondo il modello del *panspectron* teorizzato da Manuel De Landa¹⁶: non più una struttura fisica di sorveglianza, ma una rete diffusa di sensori e dispositivi che raccolgono continuamente dati su ogni aspetto della nostra vita. Questi dati vengono poi elaborati da algoritmi sempre più sofisticati, capaci di prevedere e influenzare i comportamenti futuri. Ad essere importante non è dunque tanto l'osservazione in sé, quanto la capacità di estrarre *pattern*, previsioni e *insight* dalla massa di informazioni raccolte. Infatti, non si tratta più di un'unica torre di osservazione, visibile, ma di una miriade di punti di raccolta dati disseminati nell'ambiente e per questo invisibili. Questi “sensori” non sono necessariamente dispositivi fisici dedicati, ma includono ogni interfaccia digitale con cui interagiamo quotidianamente: smartphone, computer, dispositivi IoT, telecamere di sicurezza, sistemi di pagamento elettronico, oltre che – ovviamente – profili sui social media. Mentre il *panopticon* era progettato per osservare individui specifici in spazi confinati, il *panspectron* raccoglie dati su tutto e tutti, indiscriminatamente e continuamente. Non c'è più distinzione tra sorveglianti e sorvegliati: tutti siamo parte di questo sistema di raccolta dati, spesso contribuendo attivamente (ma inconsapevolmente) attraverso le nostre interazioni digitali.

Questo meccanismo è infatti connotato da una sostanziale opacità: gli algoritmi che elaborano i dati e prendono “decisioni” sono spesso di una complessità tale da risultare incomprensibili non solo per i comuni cittadini, ma anche per molti esperti. Questa “scatola nera” algoritmica¹⁷ solleva serie questioni di trasparenza e responsabilità: come possiamo contestare o anche solo comprendere decisioni che influenzano profondamente le nostre vite se non abbiamo accesso ai meccanismi che le generano?

15. PALANO 2020.

16. DE LANDA 1996.

17. PASQUALE 2015.

Assistiamo, inoltre, a un'erosione senza precedenti della privacy e dell'autodeterminazione informativa. La raccolta pervasiva di dati personali, spesso effettuata senza una piena consapevolezza o un consenso realmente informato da parte degli individui, mina alla base il concetto tradizionale di riservatezza. Non si tratta più solo di proteggere informazioni sensibili, ma di gestire un flusso continuo di dati che, aggregati e analizzati, possono rivelare aspetti intimi della nostra personalità e condizionare i nostri comportamenti futuri. Questa perdita di controllo sui propri dati si traduce in una diminuzione dell'autonomia individuale, poiché le nostre scelte sono sempre più influenzate da sistemi che conoscono e anticipano le nostre preferenze.

Emergono così anche nuove forme di discriminazione algoritmica¹⁸, più sottili e pervasive rispetto alle discriminazioni tradizionali. Gli algoritmi, alimentati da dati che spesso riflettono pregiudizi e disuguaglianze esistenti, possono perpetuare e amplificare queste disparità in modo apparentemente neutrale e oggettivo. Decisioni cruciali in ambiti come l'accesso al credito, le opportunità di lavoro o persino la giustizia penale vengono sempre più delegate a sistemi automatizzati che possono incorporare *bias* discriminatori, spesso difficili da individuare e contestare.

Si assiste, infine, a un rafforzamento delle asimmetrie di potere. Le grandi *corporation* tecnologiche e le istituzioni che hanno accesso a vasti dataset e a sofisticati strumenti di analisi acquisiscono un potere decisionale senza precedenti¹⁹. Questa concentrazione di potere algoritmico in poche mani solleva ovvie questioni di equità e giustizia sociale, ma anche di libertà.

La libertà è stata spesso concepita principalmente come liberazione dalle costrizioni esterne. Ma nella società del controllo algoritmico sembra assai remota la possibilità stessa di affrancarci da meccanismi che modulano costantemente le nostre possibilità di scelta e che ci influenzano a un livello così sottile e pervasivo. Ciò comporta un ulteriore problema: quello della resistenza

al potere. È ancora possibile concettualizzare e mettere in pratica forme visibili e organizzate di resistenza? Come resistere a un potere che non si manifesta più attraverso ordini espliciti o coercizioni visibili, ma attraverso la modulazione delle nostre preferenze e dei nostri desideri?

Resistere alla società del controllo?

Dobbiamo a Bernard Stiegler la riflessione filosofica probabilmente più profonda sull'impatto delle tecnologie moderne sulla società, sulla conoscenza e sull'esistenza umana.

Stiegler parte dall'idea che stiamo vivendo in un'epoca caratterizzata da ciò che chiama esomatizzazione: un processo che mostra la capacità unica degli esseri umani di creare e utilizzare strumenti che estendono le loro capacità naturali, e in particolare di "esternalizzare" le sue funzioni biologiche e cognitive in strumenti tecnologici e tecniche.

Questo processo, se da un lato ha permesso un enorme progresso tecnologico e sociale, dall'altro ha portato a una crescente entropia, cioè a un disordine sistemico che minaccia la stabilità dell'ambiente e delle strutture sociali²⁰. Del resto le tecnologie, secondo Stiegler, possono essere potenti strumenti di emancipazione e di sviluppo umano, ma possono anche essere distruttive se non gestite con attenzione²¹. L'automazione, ad esempio, ha il potenziale per liberare l'umanità dal lavoro ripetitivo, ma può anche portare a una "proletarizzazione" totale, dove gli esseri umani perdono le loro competenze e la capacità di pensare criticamente, riducendosi a semplici esecutori di compiti automatizzati: Stiegler la definisce come la perdita di sapere fare (*savoir-faire*) e sapere vivere (*savoir-vivre*) a causa dell'influenza pervasiva delle tecnologie²².

Questo fenomeno non riguarda solo il lavoro manuale, ma anche le capacità intellettuali e creative degli individui, erose dalla crescente dipendenza dalle tecnologie digitali, con la conseguente perdita di capacità degli individui di partecipare attivamente e criticamente alla vita sociale e politica.

18. BARONE 2024.

19. ZUBOFF 2019.

20. STIEGLER 2015.

21. STIEGLER 2023.

22. STIEGLER 2019.

Gli algoritmi, utilizzati nei social network, nella pubblicità personalizzata e nelle piattaforme digitali, non impongono scelte in modo diretto, ma influenzano e dirigono le preferenze delle persone in modo quasi impercettibile, mortificando la loro capacità di esercitare una vera libertà²³.

In una società in cui le scelte individuali sono ormai costantemente modulate e influenzate da algoritmi, la possibilità stessa di essere liberi risulta dunque profondamente compromessa²⁴. Come è possibile resistere a un potere che non si manifesta più attraverso ordini espliciti o coercizioni visibili, ma che agisce modulando i nostri desideri e le nostre scelte? Questo tipo di potere, che Deleuze definirebbe come “società del controllo”, opera attraverso tecnologie che penetrano nella sfera psichica e cognitiva degli individui, rendendo difficile l’organizzazione di una resistenza visibile e strutturata.

Stiegler suggerisce che è necessario ripensare radicalmente le modalità di resistenza. Non è possibile resistere al potere algoritmico attraverso le forme tradizionali di opposizione, poiché questo potere è diffuso e invisibile, agendo direttamente sui processi cognitivi e affettivi delle persone. Non si tratta più di opporsi frontalmente a un potere visibile, dunque, ma di sviluppare nuove forme di resistenza: “contro-tecnologie” o “contro-ambienti” che possano riappropriarsi delle tecnologie digitali per fini emancipatori, piuttosto che lasciarle in balia delle logiche del mercato e del controllo. Questi contro-ambienti potrebbero ripristinare la capacità degli individui di pensare e agire in modo autonomo, promuovendo la riflessione critica e la consapevolezza dei meccanismi di controllo²⁵.

La resistenza al potere algoritmico non può avvenire senza un impegno nella riattivazione delle facoltà cognitive e critiche degli individui. È necessario dunque sviluppare nuove forme di soggettività e collettività attraverso un uso critico delle tecnologie digitali, promuovendo una cultura della riflessione critica che possa contrastare la riduzione della libertà individuale. Stiegler vede infatti

nella cultura e nell’educazione continua i soli strumenti in grado di contrastare la società del controllo. Il recupero della *noesis* può permettere agli individui di comprendere i modi in cui vengono influenzati dagli algoritmi e dalle tecnologie digitali, mettendoli così in condizione di reagire. Solo attraverso un approccio innovativo e consapevole alle tecnologie sarà possibile immaginare e praticare una resistenza efficace in un contesto di potere diffuso e invisibile²⁶.

La tecnologia, se non regolata da una nuova forma di sapere, può condurre l’umanità verso un destino distruttivo²⁷. È dunque necessario sviluppare una nuova epistemologia, un nuovo modo di comprendere e organizzare il sapere, che tenga conto dell’impatto delle tecnologie digitali sulla mente umana e sulla società. In questo senso, Stiegler propone una “organologia generale”: uno studio delle relazioni tra organi biologici, organi tecnici e organizzazioni sociali, come base per una nuova società che possa guidare l’umanità verso un futuro sostenibile e prospero.

La governamentalità algoritmica, con la sua capacità di prevedere e modulare i comportamenti su larga scala, sfida le concezioni tradizionali di diritti, uguaglianza e democrazia. Affrontare questi cambiamenti richiede non solo nuovi quadri normativi, ma anche nuove forme di alfabetizzazione digitale e consapevolezza algoritmica per permettere ai cittadini di reagire e influenzare attivamente il nuovo panorama sociale e politico²⁸.

È necessario sviluppare nuovi strumenti concettuali per comprendere e contestare le forme emergenti di potere che sfuggono alle categorie tradizionali di analisi. Allo stesso tempo, è fondamentale elaborare nuove forme di resistenza che possano contrastare la tendenza all’automazione del potere e alla riduzione degli individui a meri aggregati di dati. Solo attraverso una comprensione critica di questi processi sarà possibile preservare e rinnovare gli ideali di libertà e giustizia nell’era della governamentalità algoritmica.

23. ROUVROY-STIEGLER 2015.

24. STIEGLER 2021.

25. STIEGLER 2012.

26. STIEGLER 2014.

27. STIEGLER 2019-B.

28. STIEGLER 2024.

Riferimenti bibliografici

- V. BARONE (2024), *La discriminazione ai tempi dell'intelligenza artificiale: La questione algoritmica*, in Id., "Diritto e tecnologie informatiche", Wolters Kluwer Cedam, 2024
- L. BAZZICALUPO (2016), *Governamentalità: Una ri-definizione operativa della razionalità politica*, in "Pa-
rolechiave: nuova serie di Problemi del socialismo", 2016, n. 56
- L. BAZZICALUPO (2013), *Autorità. La piega di un concetto tra teologia politica e governamentalità*, in "Fi-
losofia e teologia", 2013, n. 3
- J. BENTHAM (1791/2009), *Panopticon: Ovvero la casa d'ispezione*, a cura di Michel Foucault e Michelle
Perrot, 4ª ed., Marsilio, 2009
- W. BURROUGHS (2003), *La macchina morbida*, Adelphi, 2003
- S. CHIGNOLA (2022), *Foucault oltre Foucault. Una politica della filosofia – Seminari*, DeriveApprodi, 2022
- S. CHIGNOLA (2014-A), *Foucault oltre Foucault: Una politica della filosofia*, DeriveApprodi, 2014
- S. CHIGNOLA (2014-B), *Michel Foucault e la politica dei governati: Governamentalità, forme di vita, sog-
gettivazione*, in G. Gamba, G. Molinari, M. Settura (a cura di), "Pensare il presente, riaprire il futuro.
Percorsi critici attraverso Foucault, Benjamin, Adorno, Bloch", pp. 99-137, Mimesis, 2014
- S. CHIGNOLA (2011), *Biopotere e governamentalità: Michel Foucault e la politica dei governati*, in S. Mar-
cenò, S. Vaccaro (a cura di), "Il governo di sé, il governo degli altri", :duepunti edizioni, 2011
- M. DE LANDA (1996), *La guerra nell'era delle macchine intelligenti*, Feltrinelli, 1996
- G. DELEUZE (2012), *Pourparler 1972-1990* (trad. it. S. Verdicchio), 3ª ed., Quodlibet, 2012
- M. FOUCAULT (2019), *Sorvegliare e punire. Nascita della prigione*, 26ª ed., Einaudi, 2019
- M. FOUCAULT (2005-A), *Nascita della biopolitica. Corso al Collège de France (1978-1979)*, Feltrinelli, 2005
- M. FOUCAULT (2005-B), *Sicurezza, territorio, popolazione. Corso al Collège de France (1977-1978)*, Feltri-
nelli, 2005
- E. GOFFMAN (2010), *Asylums. Le istituzioni totali: i meccanismi dell'esclusione e della violenza* (trad. it. F.
Basaglia), Einaudi, 2010
- B.-C. HAN (2016), *Nello sciame. Visioni del digitale*, 5ª ed., Nottetempo, 2016
- M. LA MONICA (2014), *Dal Panopticon di Bentham a modelli parzialmente panottici. Prigioni tra Settecen-
to e Ottocento*, Pitti, 2014
- S. LUCE (2009), *Fuori di sé. Poteri e soggettivazioni in Michel Foucault*, Mimesis, 2009
- S. MEZZADRA (2008), *Le forze e le forme: Governamentalità e bios nel tempo del capitale globale*, in A.
Amendola, L. Bazzicalupo, F. Chicchi, A. Tucci (a cura di), "Biopolitica, bioeconomia e processi di
soggettivazione", pp. 171-184, Quodlibet 2008
- D. PALANO (2020), *Bubble democracy. La fine del pubblico e la nuova polarizzazione*, Scholé, 2020
- F. PASQUALE (2015), *The black box society. The secret algorithms that control money and information*, Har-
vard University Press, 2015
- S. PIETROPAOLI (2021), *Da cittadino a user: Capitalismo, democrazia e rivoluzione digitale*, in A. Cava-
liere, G. Preterossi, "Capitalismo senza democrazia? Libertà, uguaglianza e diritti nell'età neoliberale",
Giappichelli, 2021
- A. ROUVROY (2008), *Human genes and neoliberal governance. A foucauldian critique*, Routledge, 2008

- A. ROUVROY, B. STIEGLER (2015), *Le régime de vérité numérique: De la gouvernementalité algorithmique à un nouvel État de droit*, in "Socio", 2015, n. 4
- M. SBRICCOLI (1977), *La storia, il diritto, la prigionia. Appunti per una discussione sull'opera di M. Foucault*, in "La Questione Criminale", 1977, n. 3
- B. STIEGLER (2024), *Il chiaroscuro della rete*, Kainos, 2024
- B. STIEGLER (2023), *La colpa di Epimeteo*, vol. 1, Luiss University Press, 2023
- B. STIEGLER (2021), *La miseria simbolica*, Meltemi, 2021
- B. STIEGLER (2019-A), *L'avvenire del lavoro*, vol. 1, Meltemi, 2019
- B. STIEGLER (2019-B), *La società automatica*, Meltemi, 2019
- B. STIEGLER (2015), *Platone digitale. Per una filosofia della rete*, Mimesis, 2015
- B. STIEGLER (2014), *Prendersi cura. Della gioventù e delle generazioni*, Orthotes, 2014
- B. STIEGLER (2012), *Reincantare il mondo: Il valore spirito contro il populismo industriale* (trad. it. P. Vignola), Orthotes, 2012
- P. VIRILIO (1977), *Vitesse et Politique: Essai de dromologie*, Galilée, 1977
- S. ZUBOFF (2019), *Il capitalismo della sorveglianza il futuro dell'umanità nell'era dei nuovi poteri* (trad. it. P. Bassotti), LUISS University Press, 2019



ANTONIO IANNUZZI

Metaverso, *Digital Twins* e diritti fondamentali

Metaverso e *digital twin* sono tecnologie che sembrano far ingigantire una serie di problemi giuridici che già caratterizzano il costituzionalismo digitale. Il diritto deve affrontare la regolazione del metaverso, essendo alle porte la diffusione del web 4.0: la quarta generazione del World Wide Web che, utilizzando l'intelligenza artificiale e ambientale avanzata, l'Internet delle cose, le transazioni *blockchain* affidabili, i mondi virtuali e le funzionalità XR, permette agli oggetti e agli ambienti digitali e reali di integrarsi completamente e di comunicare tra loro; promette di consentire esperienze realmente intuitive e immersive, fondendo senza soluzione di continuità il mondo fisico e quello digitale. Il saggio, partendo da un esame delle frontiere della ricerca in questi ambiti, mira ad esaminare gli effetti dell'uso di queste nuove tecnologie sui diritti fondamentali.

Metaverso – Digital twin – Diritti fondamentali – Web 4.0 – Costituzionalismo digitale

Metaverse, Digital Twins and fundamental rights

Metaverse and digital twin are technologies that seem to magnify a number of legal problems that already characterize digital constitutionalism. Law must address the regulation of the metaverse as the deployment of web 4.0 is upon us: the fourth generation of the World Wide Web, which, using advanced artificial and environmental intelligence, the Internet of Things, trusted blockchain transactions, virtual worlds, and XR capabilities, allows digital and real objects and environments to fully integrate and communicate with each other; it promises to enable truly intuitive and immersive experiences, seamlessly merging the physical and digital worlds. Starting with an examination of the frontiers of research in these areas, the essay aims to examine the effects of the use of these new technologies on fundamental rights.

Metaverse – Digital twin – Fundamental rights – Web 4.0 – Digital constitutionalism

L'Autore è professore ordinario di Istituzioni di diritto pubblico presso l'Università degli Studi Roma Tre

Questo contributo fa parte della sezione monografica *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà*, a cura di Marina Pietrangelo

SOMMARIO: 1. Tempo, diritto e tecnologie emergenti: è già arrivato il momento di avviare la riflessione giuridica sul metaverso? – 2. Il metaverso fra diritto, letteratura e *pop culture*. – 3. Il metaverso e le sfide al diritto. – 4. Metaversi e *digital twins*: le frontiere della ricerca. – 5. Metaversi e diritti fondamentali. – 5.1. *Il diritto alla salute*. – 5.2. *La proprietà*. – 5.3. *La dignità umana*. – 5.4. *La libertà di espressione minacciata da fake news e deepfakes che acquistano anche una forma (diversamente) reale*. – 5.5. *Digital divide e interoperabilità fra metaversi*. – 5.6. *Inconcepibilità dei diritti dell'avatar nei metaversi*. – 5.7. *Il diritto alla cybersecurity*. – 6. L'approccio regolatorio: quale diritto per il metaverso? – 7. Brevi suggestioni conclusive.

*Che cosa non darei per la memoria
di una strada sterrata fra muri bassi
(...)*

*Che cosa non darei per la memoria
di mia madre che contempla il mattino
nella tenuta di Sant'Irene,
ignara che il suo nome sarebbe stato Borges
(...)*

*Che cosa non darei per la memoria
di un portone di villa segreta
che mio padre spingeva ogni sera
prima di perdersi nel sonno
e spinse per l'ultima volta
il 14 febbraio del '38
(...)*

*Che cosa non darei per la memoria
di te che avessi detto che mi amavi
e di non aver dormito fino all'alba,
straziato e felice.*

(J.L. Borges, *Elegia di un ricordo impossibile*, in *La moneta di ferro*, Padova, 1996)

1. Tempo, diritto e tecnologie emergenti: è già arrivato il momento di avviare la riflessione giuridica sul metaverso?

A dispetto degli ingenti finanziamenti da parte delle Big Tech e delle più che favorevoli previsioni di sviluppo economico, il metaverso sta stentando ad affermarsi come esperienza di massa.

La promessa della fine dell'Internet a due dimensioni per via dell'affermazione della possibilità di navigare in tre dimensioni, il web 4.0, fatica, dunque, a concretizzarsi.

Le cause di questo iniziale insuccesso sono sicuramente tante: la crisi economica post-pandemica; i costi, almeno per il momento elevati, da sostenere per l'accesso a questa nuova tecnologia; alcuni nodi tecnici ancora non affrontati.

Gli occhiali AR, i visori VR e le tute aptiche oggi in commercio sono costosissime e peraltro ancora da perfezionare dal punto di vista del loro confezionamento anche in termini di prestazioni, mentre sono le tecnologie più economiche e più semplici che si diffondono velocemente.

C'è poi un problema tecnico ancora irrisolto di latenza che impedisce la diffusione di massa. È stato già segnalato che è necessario un salto quantico nell'hardware, nel software, nelle velocità di connessione, nella definizione di standard e protocolli per avere esperienze così fluide da apparire reali. La latenza indica il ritardo nell'arrivo dei dati che oggi comporta esperienze "in lieve differita". Anche la larghezza della banda, vale a dire la velocità di trasmissione dei dati, è ancora generalmente insufficiente ed influisce negativamente sulla qualità delle esperienze interattive¹.

Si avverte, inoltre, da parte dei consumatori una certa ritrosia a comprenderne funzionamento e vantaggi, mentre serpeggia un timore diffuso e un senso di possibile smarrimento relativamente all'utilizzo immersivo nella realtà virtuale aumentata. Resta ancora sullo sfondo il tema dell'alfabetizzazione informatica e del riconoscimento del diritto all'inclusione digitale che si acuisce ogni volta che si immette sul mercato una tecnologia innovativa.

Nella fase attuale di incerto sviluppo, in cui si affacciano solo come abbozzi le avvisaglie dei problemi giuridici emergenti dall'uso di questa tecnologia, è necessario, tuttavia, a parer mio, enucleare tempestivamente alcune domande di ricerca. Ne proporrò inizialmente alcune inevitabilmente generali.

La domanda di partenza attiene proprio all'opportunità di avviare una riflessione giuridica sul metaverso, benché si tratti di una tecnologia ancora in fase di esordio e non ancora largamente diffusa. In altre parole, perché è importante intraprendere ora la riflessione giuridica sul metaverso? La risposta che mi sono dato è che il metaverso intercetta quell'aspirazione di vivere una dimensione parallela che è radicata nell'esperienza umana. Non so se

avverrà già con il metaverso, ma l'*Homo technologicus* punterà a realizzare questo sogno.

Il diritto deve trovarsi pronto ad affrontare la regolazione del metaverso, essendo alle porte la diffusione del web 4.0: la quarta generazione del World Wide Web che, utilizzando l'intelligenza artificiale e ambientale avanzata, l'Internet delle cose, le transazioni *blockchain* affidabili, i mondi virtuali e le funzionalità XR, permette agli oggetti e agli ambienti digitali e reali di integrarsi completamente e di comunicare tra loro; promette di consentire esperienze realmente intuitive e immersive, fondendo senza soluzione di continuità il mondo fisico e quello digitale².

2. Il metaverso fra diritto, letteratura e pop culture

Perché l'umanità ha necessità di inventare un "metaverso"? A mio avviso la risposta dipende dalla testarda illusione che la vita, a dispetto della sua finitezza, potrebbe continuare in un "altrove". Ma anche perché l'uomo ha cercato sin dalla sua apparizione sulla Terra di liberarsi delle barriere, delle catene e dei limiti, ardendo di volare o di sconfiggere la morte; di superare l'implacabile unidirezionalità del tempo; di rivivere l'intensità di un ricordo o, semplicemente, non smarrirlo; di consentire a un non-vedente di recuperare diversamente la vista.

La letteratura ha saputo cogliere quest'aspirazione umana elaborando il concetto di universo parallelo.

Gli esempi sono innumerevoli. Su tutti, a mio avviso, vale la pena di citare il celeberrimo romanzo *La svastica sul sole* di Philip K. Dick che immagina un mondo in cui il Terzo Reich nazista ha vinto la guerra. Nel mondo parallelo costruito narrativamente da Keith Laumer nel libro *I mondi dell'Impero*, invece, i neandertaliani hanno distrutto l'*homo sapiens*³. In un dialogo dell'opera si coglie

1. Come si apprende dalla lettura di BALL 2022.

2. La definizione del Web 4.0 è fornita a livello ufficiale da Commissione europea, *Un'iniziativa dell'UE sul web 4.0 e i mondi virtuali: muoversi in anticipo verso la prossima transizione tecnologica*, doc. COM (2023) 442, 11 luglio 2023.

3. Il romanzo che narra la storia di Brion Bayard, un giovane diplomatico americano della nostra Terra che, dopo essere stato rapito dagli emissari di un altro mondo parallelo, viene convinto ad affrontare una missione su una terza Terra allo scopo di uccidere un pericoloso dittatore che si rivelerà poi essere lui stesso o, meglio, il suo doppio. Nella presentazione del libro, Sandro Pergameno, uno dei migliori curatori di collane di fantascienza, ci segnala che l'idea che sta alla base del libro è la seguente: «perché solo una linea temporale dovrebbe scoprire il viaggio paratemporale? Non ci potrebbe essere un numero svariato di culture avanzate che s'incontrano di

magnificamente questo intreccio, quando l'autore fa affermare a Brion Bayard: «Paragonata al tempo che abbiamo impiegato a evolverci dall'ameba alla scimmia (o anche dal primo homo sapiens al primo campo arato), è un attimo. Ma non rinunciare ai tuoi sogni. Sono la forza che ci porta avanti, verso la nostra meta finale... qualunque sia».

Anche nei fumetti il tema è ricorrente. L'utilizzo dei fumetti nella cultura contemporanea è affermato con forza da studiosi come Edgar Morin e Umberto Eco. In *Apocalittici e integrati*, che è una delle opere fondative del filone scientifico dedicato alla trasformazione della cultura di massa per effetto della rivoluzione di Internet, lo stesso Eco avverte nella presentazione che «quando il libro è apparso, applicare strumenti di indagine rigorosa ad argomenti come il fumetto, la canzone di consumo, la narrativa popolare, suonava, alle orecchie di molti, quasi oltraggioso»⁴. Anche la pop culture ha finalmente fatto il suo ingresso nel metodo giuridico, come dimostra il ricco ed interessante volume dal titolo *La rappresentazione delle tradizioni giuridiche nella pop culture*⁵.

Nella serie *Dylan Dog*, soprattutto, non mancano gli albi in cui sono presentate realtà di questo tipo. Una suggestiva panoramica filosofica ci offre il quadro di una serie a fumetti in cui si realizza, secondo l'autore, una sovrapposizione tra la concezione dei sogni e la teoria degli universi paralleli, che postula l'esistenza di un infinito novero di mondi possibili. La conclusione è che, seguendo gli studi avviati nella prima metà del Novecento da fisici come Niels Bohr, Werner Heisenberg o Erwin Schrödinger che diedero inizio alla rivoluzione della meccanica quantistica, la letteratura fantascientifica ha elaborato la teoria degli universi paralleli, per cui, nel fumetto citato, sarebbe «possibile immaginare che, tra tutte le nostre infinite varianti, esista una qualche forma di contatto, cioè che, una volta separate l'una dall'altra dal processo di ramificazione (...), esse continuino a essere in relazione l'una con l'altra»⁶. Come nel magnifico

libro di Michael Ende, *La storia infinita*, è la dimensione onirica del sogno a rendere possibili i collegamenti nel multiverso. In definitiva, la lettura del fumetto ci consegna l'interrogativo fondamentale: «cos'è reale davvero? A volte, la realtà di una notte ci appare tanto assurda da poter essere confusa con un sogno esattamente come accade a Dylan in *Dopo mezzanotte*», poiché pare che «la dimensione quantica sia prossima alla dimensione del sogno, rispetto al nostro universo tridimensionale»⁷.

Nella letteratura più classica, il tema dell'universo parallelo è stato toccato, tra tanti, magistralmente da Jorge Luis Borges, come vedremo.

La filosofia sul punto è sterminata ma è stata illuminata soprattutto da Schopenhauer, che nella celeberrima opera *Il mondo come volontà e rappresentazione*, argomenta «non è forse tutta la vita un sogno? – o più precisamente: esiste un criterio sicuro per distinguere sogno e realtà, fantasmi ed oggetti reali? L'unico criterio sicuro per distinguere il sogno dalla realtà è in effetti quello affatto empirico del risveglio, col quale in verità il nesso causale fra le circostanze sognate e quelle della vita cosciente viene espressamente e sensibilmente rotto», e poeticamente esprime la similitudine secondo cui «la vita e il sogno sono le pagine di uno stesso libro».

Il veloce richiamo alla letteratura non vuole essere né una divagazione né un mero esercizio retorico, ma è proficuo per documentare l'aspirazione umana ad occupare universi ultranei rispetto a quelli già abitati. I riferimenti letterari sono utili anche per sottolineare che lo sviluppo delle tecnologie emergenti – almeno fino a questo momento – è un prodotto umano e sta procedendo nella direzione in cui l'hanno inizialmente vagheggiata gli uomini, anche nella letteratura e nella fantascienza.

I grandi scrittori di fantascienza non erano solo letterati, ma anche uomini di scienza che non avevano solo una fantasia sviluppata, ma anche solide conoscenze scientifiche. Isaac Asimov, le cui leggi della robotica restano ancora insuperate perché

continuo in questo flusso attraverso i mondi paralleli? E ancora: perché confinare le nostre esplorazioni ai mondi in cui solo "homo sapiens" ha sviluppato l'intelligenza?» (PERGAMENO 1963, p. 8).

4. ECO 2011.

5. LIGUSTRO-TARCHI-RUOTOLO-MARTINICO 2023.

6. MANZOCCO 2011, p. 51 ss.

7. GIORELLO 2023, p. 22 ss.

recepite nella letteratura scientifica e giuridica mondiale contemporanea, era laureato in scienze, oltre che in letteratura e filosofia, alla Columbia University. Jin Al-Khaili, nel romanzo *Sunfall*, immagina che nel 2041 il nucleo della Terra stia per fermarsi e che gli scienziati debbano adoperarsi per salvare il genere umano. L'autore è docente di Fisica teoretica all'Università di Surrey, in Gran Bretagna, dove è titolare anche di una cattedra di comunicazione scientifica.

Quella che è stata realizzata, insomma, è la tecnologia che l'uomo è stato capace di immaginare.

Nel futuro si svilupperà una tecnologia post-umana, vale a dire che proceda secondo linee di sviluppo indipendenti dalla capacità dell'uomo di immaginarla, di supervisionarla e di realizzarla? Nella fase attuale del dibattito giuridico sul c.d. costituzionalismo digitale, che si caratterizza per l'ampia riflessione sul grado di autonomia delle macchine, eticamente accettabile per l'uomo, in un contesto di sviluppo vorticoso dell'intelligenza artificiale, si può ancora solo immaginare che queste reti neurali, quali entità autonome che già oggi creano conoscenza – perché generano linguaggio o “scoprono” nuovi antibiotici che mostrano di contrastare una serie batteri, inclusi ceppi considerati fino a qui resistenti ai farmaci – diventeranno in un futuro non così lontano talmente evolute da riuscire a produrre scoperte scientifiche indipendentemente dalla volontà dell'uomo, con modalità di funzionamento e codici tecnici di comportamento che potranno sfuggire al controllo dell'uomo.

3. Il metaverso e le sfide al diritto

La linea di sviluppo descritta nel precedente paragrafo vale anche per il metaverso che, prima è stato raccontato letterariamente da Neal Stephenson in *Snow Crash* e, dopo, è stato concepito effettivamente, senza essere (ancora) sfuggito al controllo umano.

Le questioni che pone il metaverso, allora, non possono essere sottovalutate, magari confidando nell'iniziale mancato decollo, per l'evidente ragione che reifica un'aspirazione umana. A trascurare i problemi etici e giuridici che pone si reitererebbe lo stesso errore che è stato commesso nella fase di

avvio delle piattaforme. È vero che queste ultime, diversamente, hanno avuto una diffusione rapida e imponente, ma la tardiva risposta del diritto ha fatto in modo che alcuni problemi che da principio avrebbero potuto essere affrontati con maggiore efficacia, ora sono così ingigantiti da sembrare quasi insolubili.

Personalmente penso che non sarà *solo* il metaverso a regalare all'umanità la possibilità di una vita altrove, quanto piuttosto *anche* il metaverso per effetto dell'integrazione con altre tecnologie. La storia della scienza ci dimostra che i grandi avanzamenti scientifici o tecnologici sono sempre il frutto di un incrocio, spesso inizialmente impensato, fra più tecnologie diverse⁸. L'abbraccio fra tecnologie diverse, quali il metaverso, l'intelligenza artificiale e le tecnologie per il potenziamento umano, può dischiudere scenari davvero inimmaginabili.

Come si avverte in uno studio del Parlamento europeo, *Metaverse*⁹: «Le nuove sfide del metaverso derivano dalla totale tracciabilità e dalla crescente capacità dei dispositivi VR di generare una gamma molto più ampia di dati che rivelano i movimenti, lo stato fisico, le emozioni, le capacità e i desideri dell'utente. Le cuffie e le loro periferiche potrebbero consentire l'acquisizione di un'ampia gamma di dati dell'utente, compresa l'attività neurale, come l'EEG per le interfacce cervello-computer»¹⁰. In questo momento, la c.d. *datafication*, che rappresenta la capacità di trasformare tutti gli elementi dell'ambiente circostante, inclusi gli eventi umani, le conoscenze, i contenuti, le strutture, intere città e gli spazi fisici, insieme ai movimenti in tempo reale che si verificano in essi, converte tutto in dati e informazioni che possono essere catturati, elaborati e reinterpretati dall'intelligenza artificiale. Questo processo sta attualmente avvenendo grazie all'integrazione di tecnologie emergenti, attraverso interazioni che combinano esperienze fisiche e virtuali estremamente ricche di informazioni e contestualmente potenziate.

È un fatto da considerare in prospettiva che la start up di Elon Musk, *Neuralink*, ha ottenuto dalla *Food and Drug Administration* (FDA), l'autorità di regolamentazione statunitense, l'autorizzazione a sperimentare sugli esseri umani il suo

8. Cfr. TAGLIAGAMBE 2022.

9. Lo [studio](#) citato nel testo è disponibile sul sito del Parlamento europeo.

10. Traduzione dall'inglese.

microchip che permette ai cervelli di interfacciarsi direttamente con i computer. Lo scopo principale di *Neuralink* è quello di sviluppare interfacce cervello-computer (BCI, *Brain-Computer Interfaces*) avanzate per migliorare le capacità umane e affrontare sfide legate al cervello e alle malattie neurologiche. La tecnologia di *Neuralink* mira a consentire la comunicazione bidirezionale tra il cervello e il mondo esterno. Ciò significa che i segnali elettrici provenienti dal cervello potrebbero in futuro essere letti ed interpretati dai computer, consentendo alle persone di controllare dispositivi o interagire con il mondo digitale tramite il pensiero¹¹. Le conseguenze della convergenza fra tecnologie destinate al potenziamento umano, raccolta dei dati e metaverso sono inimmaginabili. Una tecnologia come quella sperimentata da *Neuralink* sembra schiudere scenari fantascientifici che sollevano molte inquietudini se applicati al metaverso, consentendo di escogitare un modo per collegare questa nuova tecnologia direttamente al cervello umano.

Già gli sviluppi attuali di *bioengineering* applicati alla memoria consentono il c.d. *neural scanning*, che offre «la possibilità di registrare i contenuti della mente umana su un supporto digitale così come di far interagire neuroni coltivati (popolazioni neurali tenute in vita *in vitro*) con periferiche esterne che inviano un impulso elettrico a sua volta frutto della decodifica di un comando mentale»¹².

«La vita è altrove» è il verso evocativo di Arthur Rimbaud che ispirò il titolo di uno dei più bei romanzi del Novecento, di Milan Kundera. Con un soggetto diverso, l'esperienza del metaverso ci costringe ad affrontare lo stesso quel «laboratorio antropologico» nel quale Kundera si concentrava nel romanzo per rispondere alle domande fondamentali: Che cos'è l'esistenza umana? Quali esperienze vogliamo riservare esclusivamente all'uomo? Stiamo vivendo una trasformazione epocale, simile a quella che fece affermare a Kundera che «l'insieme di valori che noi consideriamo sacrosanto viene d'un colpo scardinato. Tutto diventa problematico, discutibile, soggetto all'analisi e al dubbio: il Progresso e la Rivoluzione. La Giovinezza. La Maternità. Persino l'Uomo. Ed

anche la Poesia». Non sembrano parole adatte a interrogarsi sulla straordinaria transizione digitale, biogiuridica, algoritmica a cui stiamo assistendo? Nell'appassionante romanzo di Ian McEwan, *Macchine come me*, un androide di ultimissima generazione, Adam, ha una coscienza, riesce ad essere un impareggiabile amante e si rivela un abile e prolifico compositore di haiku.

Le stesse domande fondamentali sono, allora, da porsi nuovamente oggi perché lo straordinario utilizzo dei dati, lo sviluppo dell'intelligenza artificiale, la tecnologia applicata al corpo dell'uomo e le promesse del metaverso trasmettono l'idea che siamo nel momento costitutivo e costituente del rapporto fra uomo e macchina. Questa consapevolezza, mi pare, si evince dalla *ratio* dell'art. 22 del Regolamento (UE) 2016/679, Regolamento Generale sulla Protezione dei dati personali (GDPR), che contiene i principi di una vera e propria *actio finium regundorum* fra uomo e macchina: «L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona». Se ne evince che può esserci un diritto reclamabile dall'individuo a lasciare degli spazi intangibili all'intervento esclusivo delle macchine, tratteggiando, dunque, il principio dello *human in the loop*. Questo principio si muove ora in parallelo con il diritto alla supervisione umana introdotto dall'art. 14 del Regolamento (UE) che stabilisce norme armonizzate in materia di intelligenza artificiale (*AI Act*), definitivamente approvata ed attualmente in attesa di pubblicazione.

L'ipotesi del metaverso sollecita domande ulteriori che sono il seguito di quella fondamentale. Rimaneggiando il verso di Rimbaud allora è da chiedersi: la vita è altrove? In altre parole, nello scenario distopico in cui per la prima volta osserviamo uno spazio esclusivamente digitale e altro rispetto a quello fisico – ma nel quale l'esperienza fisica o analogica e quella virtuale non sono scollegate perché il contatto avviene per via di esperienze sensoriali (*per mezzo dell'udito, della vista, del tatto e anche dell'olfatto*) – è possibile concepire

11. Sugli aspetti clinici, etici, neuroetici e giuridici di *Neuralink* è molto utile la lettura di BALCONI-IENCA-LAVAZZA et al. 2024.

12. MARCHESE 2022, p. 286, nt. 12.

l'esperienza umana oltre lo spazio fisico e la dimensione corporea, fino a tutelare un *avatar* collegato appunto attraverso i sensi umani, che ci consente di attraversare gli sconfinati spazi virtuali paralleli?

Ancora, il riconoscimento di un'ampia autonomia di agire dell'*avatar* è compatibile con l'umanesimo digitale che reclama la gran parte degli studiosi nello scenario del mondo nuovo dominato dall'intelligenza artificiale?

Utilizzando nuovamente una parafrasi, stavolta di un celebre titolo di un saggio di Stefano Rodotà, il quale poneva il nesso fra la vita e le regole¹³, il metaverso spinge la riflessione giuridica molto avanti fino a fornire lo spunto per riflettere su un possibile legame, giuridicamente sostenibile, fra la non-vita e le regole. Su questo crinale, sono davvero suggestive le riflessioni del filosofo sudcoreano Byung-chul Han sull'acquisto di senso delle non-cose e su come l'umanità stia smettendo di vivere il reale¹⁴.

4. Metaversi e *digital twins*: le frontiere della ricerca

Il metaverso è solo una delle tecnologie immersive che sono oggi disponibili. Anche per queste ragioni più che di metaverso occorre parlare di metaversi. Essi poggiano su una tecnologia di realtà aumentata e virtuale, proponendo un'esperienza molto simile al *gaming*, il cui funzionamento è legato anche all'utilizzo del *digital twin*. Le applicazioni sono già molto promettenti.

L'accesso al metaverso richiede una registrazione che permette a un utente di connettersi con la sua controparte digitale. Questa connessione digitale è garantita attraverso la condivisione delle informazioni di accesso e l'obbligo per l'utente di autenticarsi ogni volta che torna a interagire nel cyberspazio del metaverso.

I gemelli digitali riflettono le proprietà delle loro controparti fisiche perché la connessione tra gemelli virtuali e digitali avviene attraverso i loro dati.

In effetti, a proposito della convergenza tecnologica, di cui ho prima fatto brevemente cenno, la tecnologia basata sui gemelli digitali unisce e integra il mondo dell'IoT (*Internet of Things*), dell'IA (Intelligenza Artificiale) e dell'analisi dei big data. La replica digitale del mondo reale consente ai data scientist e agli specialisti di *information technology* (IT) di ottimizzare le implementazioni creando scenari ipotetici man mano che la disponibilità dei dati da inserire nel modello aumenta. Edifici, fabbriche e persino intere città sono ora rappresentate digitalmente come gemelli digitali¹⁵. Questa tecnologia si sta sperimentando anche per riprodurre interi ecosistemi naturali. Ci sono numerose ricerche finanziate per applicare la tecnologia del *digital twins* persino alla persona umana, come si vedrà nel paragrafo destinato alla tutela del diritto alla salute.

Così già oggi il gemello digitale della città, che è la chiave per la progettazione delle *smart city*, offre svariate applicazioni che consentono di monitorare e governare una città e i suoi servizi connettendo informazioni raccolte sul territorio in tempo reale, com'è stato osservato, «anche con il contributo più o meno consapevole dei cittadini»¹⁶.

Nel già citato studio del Parlamento europeo, *Metaverse*, si dà conto che l'adozione dei gemelli digitali si sta espandendo per contribuire a migliorare le decisioni e i risultati aziendali attraverso la visualizzazione e il supporto di flotte robotiche intelligenti, di operazioni di produzione complesse e di città intelligenti o persino di singoli oggetti, come un'automobile o un essere umano digitale¹⁷.

Con il progetto *Destination Earth* la Commissione europea sta collaborando con l'Agenzia spaziale europea per la realizzazione di un gemello digitale del nostro pianeta. L'ambizione è quella di realizzare una replica digitale completa entro il 2030. Attraverso una tecnologia del genere si potranno anche prevenire eventi meteorologici disastrosi.

13. RODOTÀ 2006.

14. BYUNG-CHUL HAN 2023.

15. DIETZ-PERNUL 2020.

16. PAGNANELLI 2023, p. 199.

17. Traduzione dall'inglese (p. 27).

Lo sguardo sui progetti di ricerca finanziati dall'Unione europea ci consente di anticipare la riflessione sui problemi giuridici emergenti.

L'Ue sta già investendo in iniziative importanti, come, appunto, *Destination Earth*¹⁸, *Local Digital Twins: Forging the Cities of Tomorrow*¹⁹ o *European Digital Twin Ocean*²⁰ per permettere ai ricercatori di far progredire la ricerca scientifica, alle industrie di sviluppare applicazioni di precisione e agli enti pubblici di assumere decisioni informate in materia di politiche pubbliche. La Commissione sta avviando due nuove “iniziative faro” pubbliche: *CitiVerse*, un ambiente urbano immersivo che può essere utilizzato per la pianificazione urbana e la gestione, e un *Virtual Human Twin*²¹, un essere umano virtuale gemello europeo che riprodurrà il corpo umano a supporto di decisioni cliniche e terapie personalizzate²².

Per quanto riguarda l'impatto sul mercato, un importante rapporto commerciale indica cinque categorie principali di utilizzo del metaverso da parte dei consumatori: 1) il gioco; 2) la socializzazione; 3) il *fitness*; 4) il commercio, in quanto il metaverso può essere un canale per la vendita di prodotti reali e virtuali su scala; 5) l'apprendimento a distanza che collega gruppi di individui in aule virtuali²³.

5. Metaversi e diritti fondamentali

I metaversi possono spingere molto più in avanti quella transizione – che è già stata avviata con la nascita e lo sviluppo di Internet – verso la creazione

di una copia digitale del mondo. Già, appunto, in Internet la dimensione dei diritti è ampliata e duplicata²⁴, nella dimensione metaversica questa prospettiva si esaspera fino a realizzare un mondo clonato in una dimensione persistente, non legata né allo spazio né al tempo. Ed è proprio questa la sfida principale che i metaversi pongono al diritto e alla garanzia dei diritti: il problema del superamento della dimensione del territorio e dello spazio che costituiscono il *nomos* della giuridicità.

Oltre alle questioni generali, occorre ragionare sull'impatto che l'esperienza dei metaversi esercita su alcuni diritti fondamentali. Premetto che occorrerà verificare l'incidenza sul diritto alla protezione dei dati personali alla luce dell'effettiva constatazione dei dati che saranno raccolti. Ad un primo esame, il trattamento dei dati biometrici e la possibilità di tracciare mappe cerebrali preoccupa non poco, anche nella prospettiva che si va affacciando della tutela dei neurodiritti.

5.1. Il diritto alla salute

L'introduzione di queste tecnologie è trainata senz'altro dalle promettenti applicazioni nel campo delle terapie di cura, favorendo potenzialmente il miglior godimento del diritto fondamentale alla salute. La tecnologia in parola può favorire quello che possiamo definire lo sviluppo metaversico del biodiritto, con la possibilità di ipotizzare il superamento di taluni limiti etici²⁵.

Si pensi alla possibilità di riprodurre il gemello di un organo umano o addirittura di tutto il corpo

18. V. la [descrizione](#) sul sito della Commissione europea.

19. Per un quadro, v. [Local Digital Twins: Forging the Cities of Tomorrow](#).

20. Per approfondire v. [European Digital Twin of the Ocean](#).

21. Per avere maggiori informazioni sugli obiettivi della ricerca v. [Iniziativa europea sui gemelli umani virtuali](#).

22. Ne dà notizie la stessa Commissione europea.

23. MC KINSEY AND COMPANY 2022.

24. Sulla concezione dei diritti digitali sia consentito rinviare a IANNUZZI-LAVIOLA 2023, p. 9 ss.

25. Secondo RUFFOLO-AMIDEI 2019, p. 1658 ss. «[l']intelligenza artificiale non è solo automazione produttiva, prodotti “intelligenti”, veicoli *selfdriving* e *smart contract*. È forte la corrente di chi la percepisce come la chiave per lo sviluppo – in un futuro già prefigurabile – di tecnologie di *human enhancement*. Esse, frutto della combinazione tra impiego dell'A.I., biotecnologie e scienze mediche, biomediche e genetiche, potranno essere (e già in una qualche misura sono) utilizzate per aumentare, quantitativamente e qualitativamente, le capacità fisiche e cognitive dell'essere umano o crearne di nuove, sul piano fisico, mentale ed emotivo. Il risultato è una progressiva tecnologizzazione dell'uomo, che rompe il confine tra naturale ed artificiale. Sino a travalicare le barriere della condizione umana, spaziando dal potenziamento di singole abilità fisiche dell'individuo all'incremento anche esponenziale delle capacità mnemoniche, di concentrazione e più in generale della “intelligenza”».

umano, al fine di sperimentare l'efficacia di terapie innovative sotto il profilo dell'efficacia e della tollerabilità. Il gemello digitale di un organo e del corpo umano può consentire di anticipare la diagnosi di una patologia prima della manifestazione critica della sintomatologia, così da offrire la possibilità di curare la malattia prima della sua insorgenza.

La riproduzione digitale supererà il limite del divieto di clonazione umana oggi imposto in Italia dalla legge n. 40/2004, così come diffusamente negli ordinamenti di molti altri Stati? Notevoli spunti di riflessione, in tal senso, sorgono dall'utilizzo che oggi si fa del cuore digitale: *iHeart* è un tipo di *digital twin* che realizza una replica digitale quasi perfetta del corpo umano. A differenza dei progressi raggiunti fino ad oggi, *iHeart* è in grado di riprodurre tutti i processi che avvengono nel nostro organismo. Questi processi includono i campi elettrici, la meccanica dei muscoli, la fluidodinamica del sangue e le coronarie che forniscono costantemente nutrimento all'organo²⁶. La considerazione di tutti questi processi è essenziale per comprendere il funzionamento complessivo

dell'organo, perché sono tutti strettamente correlati e non possono essere analizzati separatamente.

Spostando l'attenzione verso l'applicazione sugli animali, la loro potenziale riproduzione digitale può superare i limiti etici e i divieti legali relativi alla sperimentazione su esseri viventi?

Si porrà in futuro anche per il metaverso il possibile rischio da sottoutilizzo che molto acutamente ha posto Ugo Pagallo nel campo dell'Intelligenza artificiale applicata alla sanità²⁷? Vale a dire, a fronte delle potenzialità del ricorso alle tecnologie del metaverso, è configurabile un dovere di utilizzo. È bene chiarire che il sottoutilizzo si può configurare a fronte di un utilizzo insufficiente o parziale, «quando tale impiego parziale è dettato da ragioni sbagliate»²⁸.

Davvero impressionante è il progetto *Human Digital Twin* (HDT) che mira ad applicare la tecnologia in parola al corpo umano. Essa si basa su un decalogo che ha come punto di partenza l'idea che ogni essere umano reale avrà un corrispondente HDT memorizzato nel cyberspazio, con la dotazione di un indice unico, che può essere utilizzato come ID e come *account* per accedere all'HDT²⁹.

26. Per ragguagli è possibile consultare il sito del [progetto iHeart](#).

27. PAGALLO 2022 ha posto la questione in tal modo: «un altro problema che l'IA pone, riguarda il possibile sottoutilizzo dell'IA, cioè a dire, il mancato sfruttamento delle sue potenzialità nell'ambito medico e sanitario». Il sottoutilizzo è già all'attenzione del Parlamento europeo, come si evince da un paio di documenti citati nel volume di Pagallo. In tema v. anche OROFINO 2022, p. 158 ss.

28. PAGALLO 2022, p. 30.

29. SHENGLI 2021, p. 4. Il decalogo che riporto nella mia traduzione dall'inglese è il seguente: «1) Ognuno di noi nel mondo reale ha un corrispondente HDT memorizzato nel cyberspazio. Ognuno di essi ha un indice unico, che può essere utilizzato come ID e come account per accedere all'HDT. 2) Non appena una persona nasce, il suo HDT (supponiamo che sia un maschio) viene creato da una persona qualificata che può essere un medico, i suoi genitori o altri esperti in un ospedale o in altri istituti. L'HDT accompagnerà la persona per tutta la sua vita. Le generazioni successive della persona erediteranno alcune delle sue caratteristiche genetiche biologiche. E naturalmente eredita anche le caratteristiche genetiche biologiche dei suoi antenati. Il suo HDT può ereditare queste caratteristiche direttamente dai suoi antenati. Le persone consanguinee possono presentare malattie o caratteristiche simili, che possono essere utilizzate come base per la diagnosi. 3) Ogni persona reale e il gemello umano digitale corrispondente cambierebbero in modo sincrono. Tutti i cambiamenti della persona stessa (chiamati fattori interni, ad esempio la crescita in altezza), l'influenza su di essa (chiamata input esterno, come cure, vaccini, lesioni, ecc.) e la sua risposta (chiamata output, come stimoli, rabbia, movimento, risate, ecc.) saranno trasmessi al cyber-spazio e il Gemello Umano Digitale cambierà di conseguenza. 4) I dati di ogni esame, trattamento (farmaci, iniezioni, ecc.), immunizzazione (vaccinazione), esame fisico, ecc. nelle istituzioni mediche, che sono in forma di testo (come la registrazione della diagnosi), immagine (come l'elettrocardiogramma), numero (come la pressione sanguigna, l'altezza e il peso della persona) saranno trasportati nel cyberspazio dal personale delle istituzioni mediche con il consenso della persona reale e l'HDT aggiornerà i dati di conseguenza. 5) Alcuni attributi della persona reale, come l'età e l'altezza, aumenteranno in modo naturale e graduale e allo stesso tempo, secondo la legge della crescita umana, anche il Gemello Umano Digitale "crescerà" e potrà essere corretto dalle informazioni provenienti dalla sua controparte reale. Ad esempio, l'altezza e

Come ho già accennato, l'Ue sta finanziando progetti di ricerca che vanno in questa direzione e che, fra l'altro, potranno essere favoriti dall'applicazione del Regolamento *European Health Data Space*, appena approvato dagli organi istituzionali dell'Ue

(nel momento in cui si scrive è ancora in attesa di pubblicazione), che mira, appunto, a favorire la creazione di un ecosistema settoriale di dati sanitari all'interno dell'Unione europea.

il peso possono cambiare secondo una sorta di legge di crescita umana e possono essere raccolti ogni volta che questi dati vengono misurati e inviati al Gemello Umano Digitale da apparecchiature intelligenti. 6) Tutti i tipi di dati dei sensori indossabili, come il peso, la pressione sanguigna, il polso, la frequenza cardiaca, la respirazione, il glucosio nel sangue, il volume di esercizio e i cambiamenti emotivi, vengono inviati allo Human Digital Twin attraverso la tecnologia di comunicazione. Anche le abitudini alimentari o le ricette e le abitudini di acquisto della famiglia vengono trasmesse al gemello digitale umano per l'analisi e l'integrazione dei dati. Anche tutti i tipi di istruzione vengono importati nel Gemello Digitale Umano. Inoltre, i dati relativi all'ambiente circostante vengono inviati al cyberspazio e, di conseguenza, l'ambiente circostante nel cyberspazio cambia in modo sincrono. Se necessario, il gemello digitale dell'ambiente circostante può essere costruito nel cyberspazio. Questo gemello digitale dell'ambiente circostante è solo l'ambiente circostante. Alcune informazioni devono mantenere la coerenza tra i relativi HDT e dintorni. Se il cambiamento di alcune informazioni può rompere la coerenza, è necessario introdurre la tecnologia a catena di blocchi per tracciare il cambiamento delle informazioni ed eliminare l'incoerenza, in modo che i dati correlati tornino ad essere coerenti. 7) Il Gemello Umano Digitale può utilizzare una serie di dati e informazioni per valutare la situazione umana e fornire pareri di valutazione alla persona reale e agli ospedali ad essa collegati. Con l'aiuto di sistemi di conoscenza esperti, vengono effettuate valutazioni della salute e diagnosi di malattie e le informazioni vengono restituite agli utenti. Le tecnologie interessate comprendono l'analisi dei Big Data, l'Edge Computing, l'Internet degli oggetti, la fusione dei dati, la diagnosi intelligente, l'analisi dei cluster, la rete neurale artificiale e l'albero decisionale e così via. I risultati della valutazione dello stato di salute saranno trasmessi alla persona reale e ai suoi medici in ospedale sotto forma di previsione, suggerimento, guida, allarme o programma di trattamento. Queste informazioni consentono alla persona reale di apportare determinati miglioramenti, come rafforzare l'esercizio fisico, migliorare la struttura alimentare, proseguire il trattamento, ecc. In caso di emergenza, l'ospedale invierà immediatamente un'ambulanza e verranno adottate misure di primo soccorso. 8) Una o più persone autorizzate possono accedere al suo sistema Human Digital Twin per esaminare i contenuti. Grazie alla tecnologia VR/AR, il sistema è in grado di fornire una vivida immagine 3D della persona reale e di visualizzare la situazione sanitaria in modo dinamico e visivo. Si possono persino osservare i suoi organi interni, generati dalla tecnologia di ricostruzione 3D. 9) Per mantenere la privacy, è possibile utilizzare password, impronte digitali, riconoscimento dell'iride, login autorizzato, crittografia a catena di blocchi, autenticazione, identificazione e altre tecnologie per la crittografia al fine di evitare manomissioni. Ogni HDT necessita di un account e di una password per l'accesso e la visualizzazione. Per gli adulti, l'account e la password possono essere controllati da loro stessi. Per i bambini, l'account e la password possono essere controllati dai genitori o dai tutori. Se necessario, i medici o i professionisti possono essere autorizzati a consultarlo o a modificarlo. 10) Altri meccanismi di sicurezza: per l'accesso fidato, le istituzioni mediche e i singoli individui devono effettuare l'autenticazione dell'identità e il rilevamento delle vulnerabilità per accedere al sistema HDT. Per una connessione di comunicazione sicura e affidabile, sono necessarie l'autenticazione dell'indirizzo reale e la trasmissione e l'autenticazione di percorsi fissi, ovvero gli indirizzi IP delle istituzioni mediche e delle abitazioni sono solitamente fissi e devono essere registrati; il percorso di comunicazione e il percorso di routing sono solitamente fissi. Per un accesso sicuro e affidabile ai dati, è necessario utilizzare l'Edge Computing e il controllo di accesso cross-line per garantire la sicurezza dell'accesso ai dati. Ora le istituzioni mediche, le famiglie e i nodi di dati personali dispongono di potenza di calcolo e capacità di archiviazione e possono eseguire algoritmi di sicurezza per garantire la sicurezza e la verifica. Per garantire l'affidabilità, le istituzioni mediche, le famiglie, i dispositivi dei nodi, i dispositivi di routing e i terminali personali devono essere registrati e l'identità di ciascun indirizzo è incorporata nell'indirizzo per la tracciabilità. Dopo aver ascoltato l'assegnazione dell'indirizzo nella rete di accesso, l'IP del dispositivo e la porta di comunicazione sono legati dinamicamente per realizzare l'affidabilità dell'indirizzo di origine».

5.2. La proprietà

Il diritto che immediatamente sembra essere travolto dalla trasformazione metaversica è quello della proprietà: il metaverso quindi pone un'altra sfida all'«enigma della proprietà»³⁰. Dalla concezione materiale *usque ad sideros*, alla dimensione del godimento pieno ed esclusivo su un bene, passando per la funzionalizzazione sociale imposta dalla Costituzione italiana e dalle successive tensioni soprattutto con la Convenzione Europea dei diritti dell'uomo, ora il metaverso pone la dimensione della derealizzazione³¹ dei beni del mondo oggetto di proprietà se non della necessità di ripensare la proprietà scollegata da un bene tangibile. Al riguardo, molto efficacemente già si è parlato di «tokenizzazione sui diritti di proprietà», a sostenere la seguente questione problematica: «i token (digitali), in quanto tali, a prescindere dal fatto che rappresentino un asset finanziario o non-finanziario, possono essere fatti oggetto di un diritto di proprietà? In altri termini, i token sono suscettibili di appropriazione in senso tecnico, ovvero il rapporto tra colui che, sulla base del registro distribuito, appare il legittimo titolare dei token, e il token stesso, è riconducibile al diritto di proprietà?»³². Com'è stato condivisibilmente proposto da altra attenta dottrina: «tutti i beni presenti nel metaverso, allora, possono assurgere al rango di beni giuridici e costituire, sulla scorta della definizione dell'art. 810 c.c., oggetto di diritti»³³.

5.3. La dignità umana

Il metaverso rischia di diventare uno specchio deformante dell'identità personale, intesa come diritto ad essere se stesso³⁴: è un sistema persistente

che si resetta ma non finisce, perché continua a esistere a prescindere dall'interazione dell'utente. È «vivo» perché prosegue in tempo reale per tutti gli utenti.

Senza dubbio, il metaverso potenzialmente riscrive di contenuti nuovi la dignità umana, l'identità personale, ma anche la cittadinanza che, nell'accezione digitale, si scollega dalla cittadinanza nazionale staccandosi dalla territorialità statuale. L'allarme è stato già opportunamente sollevato: «La prevalenza della realtà virtuale potrebbe facilmente condurre ad un nuovo assalto silente alla vulnerabilità umana esposta alla modulazione comportamentale degli utenti/consumatori, aprendo a diverse questioni di giustizia sociale, di mercificazione dei dati personali e di pratiche predatorie e aggressivamente profilatorie, senza contare che alla perdita di autonomia segue la perdita di libertà, la disintegrazione dell'identità personale e, quindi, la violazione della dignità»³⁵.

Il metaverso segna, com'è stato detto, un passo ulteriore nella fase di «shock antropologico» che è già sospinto dall'avvento della globalizzazione e dall'avvento dell'intelligenza artificiale³⁶.

L'aspetto che preoccupa di più è la scomposizione e la disarticolazione del concetto di realtà e del canone di verità che si andranno a determinare. Un'identità personale multipla, analogica e digitale non consentirà di stabilire con chiarezza la natura dell'interlocutore, umano o virtuale, come neppure la matrice dell'identità personale. Davvero lo sviluppo del metaverso porrà il dilemma di accertare il «chi sono»: sono la persona fisica od anche il mio *avatar*?

30. RODOTÀ 1990, p. 16.

31. «L'ordine digitale *derealizza* il mondo *informatizzandolo*» BYUNG-CHUL HAN 2023, p. 5.

32. DE CARIA 2021, p. 92.

33. A questa conclusione perviene condivisibilmente RICCIO 2023, p. 89.

34. Come ha affermato la Corte costituzionale nella sent. n. 13/1994, è possibile annoverare il diritto all'identità personale «tra i diritti che formano il patrimonio irrinunciabile della persona umana», ai sensi dell'art. 2 della Costituzione. Questo riconoscimento postula in concreto l'esistenza del «diritto ad essere sé stesso, inteso come rispetto dell'immagine di partecipe alla vita associata, con le acquisizioni di idee ed esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano, ed al tempo stesso qualificano, l'individuo». Nella letteratura sterminata in tema si segnala, da ultimo, ALPA 2021. Sul rapporto fra identità personale e digitale è fondamentale almeno la lettura di RESTA 2007, p. 211 ss.

35. CERRINA FERONI 2023, p. 10.

36. Così MAZZARELLA 2022, p. 5.

Nella prospettiva delle attività personali nel metaverso il probabile superamento di alcune barriere etiche – come dicevo prima – porrà la questione della diversa gradazione della dignità umana. Un *avatar* con contatto sensoriale umano potrà tenere comportamenti vietati nel mondo fisico dalla legge penale. Si è già verificato il caso di uno “stupro” nei confronti dell'*avatar* di una donna che sta già mettendo alle corde l'applicazione del diritto penale³⁷. Non mi soffermo su questo profilo, se non per segnalare la tesi di chi ricostruisce queste attività come prevalentemente interne alla dimensione del *gaming*. Per parte mia, tuttavia, osservo che il maggiore coinvolgimento emotivo dell'agente rispetto all'esperienza del gioco consiglia di non limitare ogni aspetto a questa dimensione³⁸. Ma pone dilemmi etici anche la possibilità di ripetere azioni nel metaverso che sono l'essenza dell'umanità: la genitorialità, l'intimità. La dignità umana è così destinata potenzialmente ad affievolirsi fino a scendere sotto un livello di tutela minima. È ancora un uomo quello che replica per mezzo del suo gemello digitale azioni essenzialmente e intimamente umane?

Il metaverso può provocare insieme alla perdita dell'unicità e irripetibilità di ogni singola esperienza umana, la confusione o lo smarrimento della realtà: in effetti, sposta l'esperienza su una realtà virtuale, perciò opera in parallelo rispetto alla realtà materiale. Molti autori fanno notare che anziché di realtà virtuale sarebbe più corretto parlare di realtà aumentata, dal momento che questa tecnologia consente di arricchire la nostra esperienza sensoriale sul piano visivo, uditivo e in prospettiva non solo. La connessione fra realtà materiale e metaverso sarà, perciò, evidente. Quest'esperienza sarà, poi, continua, a differenza delle altre che sin qui ha favorito Internet. Tant'è che in questo ecosistema, il diritto alla disconnessione³⁹ – che pure si fa fatica a rendere compatibile con un'esperienza

persistente e immersiva – può finire per configurarsi come un diritto (o un ritorno) alla realtà materiale.

5.4. La libertà di espressione minacciata da *fake news* e *deepfakes* che acquistano anche una forma (diversamente) reale

Nei metaversi si può verificare che la piattaforma privata imponga obblighi specifici di *moderazione dei contenuti* che limitino la libertà di espressione o i comportamenti che può tenere l'*avatar*⁴⁰. Sotto questo profilo, i gestori dei diversi metaversi sono da ricomprendersi fra i soggetti che sono destinatari degli obblighi di cui all'art. 14 del Regolamento 2022/2065, c.d. *Digital Services Act* (DSA)⁴¹.

L'esperienza dei metaversi, tuttavia, non appare pienamente riducibile a quella delle piattaforme perché aumenta esponenzialmente il pericolo di costruire delle verità alternative. Nei metaversi se già si mette in dubbio l'idea della realtà, sembra ancor di più appassire la concezione della verità, scomposta e devastata tra realtà e finzione, fra ambiente analogico e digitale, tra percezione sensoriale elaborata dal cervello umano e percezione filtrata dalla realtà aumentata. Già oggi la bulimia informativa (e pseudoinformativa) offerta dal web e dalle *Internet Platforms* mette in crisi la capacità di discernere il vero dal falso, conferendo la stessa forma al reale e alla finzione. Con la realtà aumentata del metaverso la capacità di discernere il vero dal falso e – quello che a me appare ancora più preoccupante – il reale dalla finzione del doppio digitale rischia di annebbiarsi ancora. Si avverte specialmente il rischio di una possibile difficile coesistenza fra una “verità reale” e una “verità digitale”, con la seconda che può assumere anche i contorni illusori di una forma tridimensionale, ancor più simile alla prima.

Il tema del *fake* è esploso nell'età delle piattaforme, sia come *fake news* sia come *deepfakes*, sia come *deepnude*⁴², soprattutto in raffronto con la

37. Sul rilievo eventualmente penalistico dei fatti che avvengono nei metaversi v. FIORE-RESTA 2023, p. 109 ss.

38. V. RUFFOLO 2023-A, p. 125 ss.

39. Sulla rilevanza costituzionale del diritto alla disconnessione e sulla sua applicazione nell'ambito del lavoro agile v. PRETEROTI 2023, p. 1 ss.; ZOPPOLI 2023.

40. Cfr. RUFFOLO 2023-A, p. 129 ss. In generale, su questi aspetti v. BUCALO 2022.

41. Per approfondimenti su questi obblighi v. OROFINO 2024-A, p. 143; LONGO 2023, p. 737 ss.

42. In tema la letteratura è sterminata, ma per il taglio che si propone nel testo cfr. RUFFOLO 2023.

libertà di espressione⁴³. I metaversi, con la offerta di realtà aumentata, possono riempire di forma, di sostanza, di esperienze tangibili ai sensi e di contenuti la diffusione di verità “alternative” o di notizie o immagini o suoni falsi, che diverrebbero ancora più difficilmente distinguibili dal vero.

Sembra ancora più preoccupante in questa prospettiva la tutela del libero convincimento delle opinioni politiche e della libertà del voto, a fronte del pericolo di generazione di contenuti personalizzati, manipolati ad arte per essere offerti in pasto a soggetti la cui mappa cerebrale sia stata pienamente tracciata e, magari, anche riprodotta.

La libertà di autodeterminarsi che è il gradiente della partecipazione politica può essere grandemente inquinata in questo ecosistema in cui la mente può essere addomesticata o l'informazione può essere moderata o censurata.

Insomma, anche con quest'ultima considerazione fatalmente si torna alla tesi di Schopenhauer da cui eravamo partiti: «la vita e il sogno sono le pagine di uno stesso libro». Affrontare per tempo questi problemi può servire a evitare di trasfigurare il sogno in un incubo anti-democratico.

5.5. Digital divide e interoperabilità fra metaversi

Un posto centrale negli studi giuridici sul metaverso occupa il problema del diritto di accesso alla tecnologia emergente, che è una manifestazione contemporanea del principio costituzionale dell'uguaglianza sostanziale. Nella prospettiva di una diffusione massiva della tecnologia, attualmente l'accesso è grandemente impedito, come già detto, dall'elevato costo dell'hardware necessario. Si pone, quindi, anche in questo ambito il tema del *digital divide*.

La difficoltà nell'apprendere l'uso di questi strumenti, con piena consapevolezza dei rischi e delle opportunità, pone anche la questione dell'acquisizione di un'educazione e di una cultura digitale che possano garantire il diritto alla fruizione e poi all'utilizzo informato della nuova tecnologia di cui discutiamo.

Un altro problema che si pone, come se i precedenti non bastassero, è quello dell'interoperabilità fra i tanti metaversi che avranno, come la storia della tecnologia dimostra, standard tecnici diversi che non consentiranno, con ogni probabilità, tale fruizione all'utente. Dovrà essere portato avanti, perciò, ogni tentativo di individuare standard unici che consentano l'interoperabilità fra le piattaforme proprietarie private⁴⁴ e che assicurino allo stesso tempo il godimento di tutta una serie di altri diritti strumentali come soprattutto, *ictu oculi*, la portabilità dei dati. Si pensi al caso di un soggetto che investe in un metaverso che poi magari cesserà di operare: che fine farà la sua esperienza? E i suoi denari e le proprietà acquisite? Questo rischio si avverte paradossalmente proprio in considerazione delle sbandierate caratteristiche dei metaversi, che promettono, invece, di consentire un'aumentata possibilità di interconnessione tra persone e tra esperienze, grazie alla capacità di rendere i suoi spazi interoperabili⁴⁵.

Sull'effettiva garanzia d'interoperabilità fra i metaversi si gioca una partita davvero importante per il successo di questi mondi: deve essere riconosciuto pienamente il diritto alla portabilità che postula l'effettiva possibilità di trasferire altrove il bene su cui insistono i diritti reali. Occorre tenere in grande considerazione che in questi ambienti virtuali una serie di rischi sono reali⁴⁶.

43. In tema fra i tanti v. almeno COLAPIETRO 2022; MAGNANI 2018. Sulla libertà di espressione sono fondamentali le letture di PACE-MANETTI 2006 e di ESPOSITO 1956.

44. Sul problema che comporta per la *net neutrality* la centralizzazione della governance del metaverso in capo ad alcune imprese private NAZZARO 2023, p. 55 ss.

45. Così FLORIDI 2022, spec. p. 4.

46. Cfr. RICCIO 2023, che si chiede opportunamente: «Se acquisto un quadro nel mondo reale, posso portarlo dove voglio, con i soli limiti eventuali delle disposizioni imposte dalla normativa in materia di beni culturali all'esportazione di tali beni; se acquisto un quadro in NFT, lo stesso è automaticamente “importabile” e commercializzabile in tutte le piattaforme? Stando al complesso di regole attualmente esistenti, la risposta non può che essere di segno negativo. Il rischio per gli utenti, quindi, potrebbe essere quello di fare degli investimenti ingenti e poi di essere colpiti dalla “volatilità” del bene acquisito, che potrebbe – ipotesi estrema – non essere

5.6. Inconcepibilità dei diritti dell'avatar nei metaversi

A questo punto, poste queste domande, è necessario sgombrare il campo da un equivoco che è costituito dalla pretesa di riconoscere diritti all'*avatar*.

Per riflettere sul punto occorre partire dall'eventuale riconoscimento della personalità giuridica dell'*avatar* e dalla connessa possibilità di imputazione della responsabilità giuridica, posto che «il problema si pone con più forza laddove si comprenderà se l'*avatar* può agire indipendentemente dalla persona umana a cui si riferisce (processo forse reso possibile attraverso lo sviluppo del deep learning)»⁴⁷.

Il punto davvero centrale da cogliere perché orienta la formazione del convincimento a favore o meno della concepibilità dei diritti dell'*avatar* è quello relativo al riconoscimento della coscienza dell'*avatar*⁴⁸.

Anche su questo aspetto il cinema offre un'affascinante suggestione. Mi riferisco al film *Nirvana* di Gabriele Salvatores nel quale in un mondo tecnologicamente più avanzato, il protagonista, Solo, che per effetto dell'infezione di un virus digitale acquista coscienza di sé, prende consapevolezza di essere nulla più che il personaggio di un videogioco ambientato in una dimensione che oggi appare molto simile al metaverso. Nel finale poetico e struggente, Solo chiederà a Jimi, il suo programmatore pentito e in crisi, di essere cancellato per scomparire insieme al gioco nel quale è intrappolato e in cui ripete ossessivamente comportamenti in un ambiente claustrofobico analogo all'angusto acquario di un pesce rosso. Il finale evoca la rivedicazione, da parte del personaggio virtuale, di un

diritto alla cancellazione («Cancellami Jimi», chiede Solo), così da poter essere almeno condannato a svanire come «un fiocco di neve che non cade in nessun posto».

Tornando alla tecnologia dei nostri giorni, si tratta di riflettere sul fatto che alcuni ordinamenti giuridici riconoscono diritti anche a soggetti che non sono persone umane. Pensiamo soprattutto alle norme dell'ordinamento giuridico tedesco che riguardano la protezione degli animali: le stesse potrebbero essere applicate anche ai robot o agli *avatar*? A questi ultimi possono essere riconosciuti addirittura dei diritti che il diritto oggettivo attribuisce agli umani?

Nella letteratura scientifica vi è un consenso abbastanza robusto nel sostenere la tesi che nega che computer e robot abbiano proprietà mentali. Né sono state ancora avanzate tesi tendenti a riconoscere a robot, *avatar* o a sistemi di intelligenza artificiale la capacità di provare sensazioni o di soffrire. Se, invece, dovesse provarsi in futuro che essi abbiano una coscienza dovremmo immediatamente regolare diversamente l'utilizzo di questi sistemi e riconoscere a loro la garanzia dei diritti fondamentali⁴⁹.

Non può neppure dirsi che nella direzione di riconoscere diritti alle macchine proceda la direttiva sul c.d. "diritto alla riparazione" (Directive of the European Parliament and of the Council on common rules promoting the repair of goods and amending regulation (Eu) 2017/2394 and directives (Eu) 2019/771 and (Eu) 2020/1828) per i consumatori approvata da ultimo dalla Commissione europea, perché appare piuttosto tendente a riconoscere i diritti dei consumatori nei confronti di fenomeni tipici del consumismo tecnologico

importabile in nessuna piattaforma oppure – ipotesi più realistica – essere deprezzato per l'impossibilità di importarlo in una piattaforma che ha acquisito importanti posizioni di mercato».

47. Come si legge in SARZANA DI S. IPPOLITO-PIERRO-EPICOCO 2022, p. 32 ss.

48. In senso diametralmente opposto si è espresso, per esempio, CHEONG 2022.

49. NIDA-RÜMELIN-WEIDENFELD 2018, § 2 (*Posso aiutarla, signore? I robot come nuovi schiavi digitali*), notano che «alcuni sostenitori dell'Intelligenza Artificiale difendono la tesi che in sostanza non si possa fare alcuna differenza tra un cervello umano e un computer. Giuristi e sociologi sono messi sempre più a confronto con la questione relativa all'imputabilità di errori ai (futuri) robot, ossia alla possibilità di attribuire loro una responsabilità giuridica. Negli istituti internazionali di ricerca i giuristi si domandano se i robot vadano considerati come meri strumenti dei quali devono rispondere i loro possessori o i loro produttori, oppure se essi, in un futuro non ben definito, a seconda del grado di autonomia che avranno raggiunto, dovranno godere di uno status speciale che attribuisca loro una responsabilità, ma anche dei diritti. In conclusione, recita così l'argomento sotto il profilo giuridico, anche i robot avrebbero dei doveri ai quali adempiere».

come l'obsolescenza programmata o la frenetica sostituzione di prodotti in luogo della riparazione. Neppure il riconoscimento della cittadinanza dell'Arabia Saudita, nell'ottobre del 2016 a un androide, Sophia, con volto e corpo dalle fattezze femminili in grado di replicare diverse espressioni facciali umane sembra andare nella direzione del riconoscimento dei diritti e dei doveri, apparendo piuttosto come un fatto di folklore e di clamore pubblicitario-mediatico creato ad arte.

5.7. Il diritto alla cybersecurity

L'esperienza nei metaversi deve essere sicura, per tutte le possibilità e i rischi che genera⁵⁰.

Nel libro *Our Final Invention* di James Barrat viene illustrato come l'ecosistema cibernetico potrebbe essere sfruttato per attacchi informatici, anche da parte di attori economici⁵¹ o, aggiungo io, politici. Nell'ecosistema digitale, possono essere condotti giochi di guerra informatici (come *Cyberwars* e *Cyber Shockwave*), in cui si creano scenari di disastro allo scopo di addestrare l'utente a trovare soluzioni. Nel libro, Barrat sostiene che le frodi finanziarie producono danni ingenti che, in termini di dimensioni finanziarie, possono essere paragonate agli attacchi terroristici. Tra le applicazioni più utili vi è il *Cyberrange* che è uno strumento che permette di fare training ai dipendenti di un'azienda in modo efficace: stressando la postura di sicurezza del proprio network costantemente tramite digital twin totale o ibrido, creando scenari complessi o predisponendo sessioni di gaming, così da affrontare la cybersecurity in modalità "gioco" quindi più facilmente comprensibile da utenti meno abili o predisposti.

Nello studio del Parlamento europeo sul metaverso, più volte citato, si chiarisce che, come tutte le tecnologie, quest'ultima può avere un utilizzo bifronte, con applicazioni sia pacifiche che militari o con usi e rischi eticamente accettabili o meno: «allo stesso modo in cui l'IA può essere utilizzata

per alimentare armi autonome, i metaversi possono essere utilizzati per creare versioni digitali di spazi e persone considerate avversarie. Questo permette il monitoraggio in tempo reale di tali spazi e persone utilizzando satelliti e l'Internet delle cose, compresi i loro dispositivi mobili. Può essere utilizzato per eseguire diversi scenari, addestrare e dispiegare armi. Questa utilità del metaverso può anche interessare i servizi di intelligence e le forze di polizia. Ciò solleva preoccupazioni sulla sorveglianza, che può avere un impatto sulla democrazia e sui diritti individuali, superando quelli derivanti dall'uso di software spia come Pegasus».

Perciò sono notevoli le potenziali applicazioni del metaverso anche in campo militare, potendo essere utilizzato come strumento per creare ambienti sintetici unici (SSE), che offriranno una comprensione globale della situazione: «la creazione di una replica sintetica di un ambiente operativo, sia per scopi di difesa e sicurezza interna che per la deterrenza e l'intervento in un'area di responsabilità più ampia, consentirà alle diverse unità e forze combinate di ottenere migliori prestazioni, addestrarsi in modo più realistico ed efficiente e sostenere trasformazioni più ampie, come l'integrazione di forze equipaggiate, non equipaggiate e autonome».

La NATO e i *think tank* come il Consiglio Atlantico hanno manifestato più volte l'opportunità ed anzi la necessità di usufruire di ambienti virtuali o di ambienti sintetici per scopi militari⁵². Ad esempio, si legge ancora nel menzionato rapporto dell'Ue che è stato creato un ambiente sintetico unico e completo per l'Estonia.

Sono evidenti, per quanto detto, le notevoli applicazioni dei metaversi alle politiche di sicurezza e militari. Ma le stesse applicazioni possono anche essere utilizzate per scopi non difensivi e pacifici. Per questi motivi, l'Ue raccomanda di migliorare la resilienza ai cyberattacchi, contribuendo ad aumentare la consapevolezza del rischio e la conoscenza dei processi di cybersecurity⁵³.

50. CERRINA FERONI 2023, p. 29: «Già oggi, a fronte di metaversi non ancora interoperabili, rimane fondamentale garantire l'utilizzo delle più aggiornate misure di sicurezza e di una metodologia certa nell'ambito della gestione dei data breach, considerato altresì che la realtà virtuale immersiva potrebbe generare nuove fonti di illeciti».

51. BARRAT 2013, p. 155.

52. Come apprendo dalla lettura di RICHMAN-PITMAN-NANDAKUMAR 2022/2023.

53. L'obiettivo è dichiarato nella già citata comunicazione "Bussola digitale 2030", del 14 dicembre 2022, che istituisce il programma politico del Decennio digitale 2030 e stabilisce gli obiettivi generali della politica digitale fino al 2030.

Di conseguenza, anche le norme che avranno ad oggetto i metaversi dovranno raccordarsi con tutte le fonti derivate dell'Ue nonché con le fonti nazionali di recepimento in tema di *cybersecurity*, che sono ormai davvero cospicue⁵⁴.

6. L'approccio regolatorio: quale diritto per il metaverso?

Una delle questioni che pongono le tecnologie digitali emergenti e le piattaforme è quella relativo all'individuazione del tempo ottimale per la regolazione.

Ho argomentato in altra sede⁵⁵ che l'esempio che, a tal proposito, ci ha offerto l'approvazione del Regolamento sull'intelligenza artificiale (*AI Act*) è emblematico se si pensa che la proposta inizialmente era stata criticata perché, ad avviso di alcuni, introduceva una disciplina dell'intelligenza artificiale troppo prematuramente rispetto allo stato della sua diffusione, salvo dopo pochi giorni a seguito del clamore generato per la diffusione dell'intelligenza artificiale generativa basata su *Large Language Model*, ChatGPT di Open AI per prima, criticare i tempi lunghi per l'adozione regolamento che sarebbe stato ormai tardivo, in quanto le norme ivi contenute sarebbero state già obsolete prima ancora di essere state approvate. Troppo tardiva è apparsa, ancora, l'adozione del DSA e del DMA rispetto alla travolgente ascesa delle piattaforme. Troppo presto, invece, si dice, possa arrivare una possibile regolazione dei metaversi. Insomma, sorge in questi casi l'esigenza di individuare il momento ottimale in cui adottare una direttiva o un regolamento, anche in considerazione dei tempi lunghi non solo di approvazione degli atti, ma ancor prima di concepimento e di confezionamento delle proposte.

Nella comunicazione del 9 marzo 2021 intitolata *Bussola digitale 2030: la via europea per il decennio digitale* (la "Comunicazione sulla Bussola digitale"), la Commissione ha delineato la sua visione per il 2030, volta a potenziare i cittadini e le imprese attraverso la trasformazione digitale, indicando in particolare il "governo come piattaforma",

come un nuovo modo di costruire i servizi pubblici digitali, che fornirà un accesso olistico e facile ai servizi pubblici con un'interazione senza soluzione di continuità di capacità avanzate, come l'elaborazione dei dati, l'IA e la realtà virtuale; fornendo un piano che probabilmente influenzerà l'iniziativa sui mondi virtuali e lo sviluppo del metaverso in Europa.

Il 14 febbraio 2022, la Presidente *protempore* della Commissione UE, Ursula von der Leyen, ha annunciato lo sviluppo, tra le nuove iniziative chiave per il 2023 – nel quadro di un'Europa adatta all'era digitale – di un'iniziativa sui mondi virtuali, come il metaverso, basata sul rispetto dei diritti digitali e delle leggi e dei valori dell'Ue. L'obiettivo è quello di creare mondi virtuali aperti, interoperabili e innovativi che possano essere utilizzati con sicurezza e fiducia dal pubblico e dalle imprese⁵⁶.

L'11 luglio 2023, di conseguenza, la Commissione ha adottato una nuova Strategia sul web 4.0 e i mondi virtuali per guidare la prossima transizione tecnologica e garantire ai cittadini, alle imprese e alle amministrazioni pubbliche dell'Ue un ambiente digitale aperto, sicuro, affidabile, equo e inclusivo.

La Strategia poggia su quattro pilastri.

Il primo punta a responsabilizzare le persone e rafforzare le competenze per promuovere la consapevolezza e l'accesso a informazioni affidabili e creare un bacino di talenti di specialisti del mondo virtuale.

Il secondo è dedicato alle imprese e mira a sostenere un ecosistema industriale web 4.0 europeo per alimentare l'eccellenza e avviare alla frammentazione.

Il terzo è rivolto alla pubblica amministrazione con l'obiettivo di sostenere il progresso sociale e i servizi pubblici virtuali per sfruttare le opportunità che i mondi virtuali possono offrire.

Il quarto guarda all'aspetto regolatorio ed è finalizzato a definire standard del web 4.0 in linea con la visione e i valori dell'Ue, condivisi a livello mondiale, che siano aperti e interoperabili, impedendo

54. Per un'analisi approfondita v. ora LONGO 2024, p. 53 ss.

55. Il riferimento è a IANNUZZI 2024, p. 21.

56. Cfr. *Metaverse*, Study requested by the European Parliament JURI Committee, 2023, p. 81.

che questi ambienti siano dominati da pochi operatori di grandi dimensioni⁵⁷.

Relativamente all'approccio regolatorio, dal punto di vista sostanziale si pone innanzitutto il problema di valutare che la disciplina sui metaversi, che sono piattaforme aventi natura privata e proprietaria⁵⁸, dovrebbe coordinarsi con le norme dettate dal DSA e dal DMA⁵⁹, ma anche con tutti i regolamenti e le direttive copiosamente adottate dall'Ue per la regolazione degli altri oggetti della società digitale (dati, intelligenza artificiale, sicurezza cibernetica), evitando di incorrere in antinomie. Prendendo preliminarmente in considerazione la ricca disciplina già esistente e, soprattutto, i principi che se ne ricavano sarà ancora necessaria e opportuna l'adozione di un regolamento o di una direttiva europea precipuamente dedicata ai metaversi⁶⁰? E quali Autorità pubbliche saranno chiamate a garantire l'effettività dei diritti fondamentale in queste arene digitali⁶¹?

Oltre le fonti derivate dell'Unione europea si apre poi lo spazio delle norme tecniche, private o armonizzate.

Se già il concepimento degli standard tecnici relativi all'utilizzo dell'intelligenza artificiale sta

alimentando un'accesa contesa geopolitica globale, è facilmente prevedibile che la stessa partita si giocherà sul piano dell'individuazione degli standard tecnici concernenti i metaversi⁶². In un ambiente digitale globale, com'è stato affermato, i rischi «per il principio dello Stato di diritto non provengono solo dall'attuazione di tecnologie digitali da parte di attori pubblici, ma anche, e principalmente, dalla capacità degli attori privati trans-nazionali di sviluppare e applicare standard privati in concorrenza con valori pubblici»⁶³.

Si tratta di un ambito di regolazione che ha ad oggetto una «realità immersiva che consente a numerose innovazioni digitali di svilupparsi in un habitat ideale, non da ultimo per il fatto che il loro funzionamento prescinde dalla presenza dello Stato»⁶⁴ ed in cui i poteri pubblici sembrano aver perso ogni ruolo e rischiano anche di smarrire ogni aspirazione ad assumerne uno in futuro. In proposito è stato ben affermato che «Ad oggi, invece, il rischio che si prospetta sempre più reale di fronte all'assenza dei poteri pubblici nel metaverso è quello del ritorno ad una sorta di forma di stato patrimoniale di stampo (neo)feudale, un *medioverso* in cui i grandi proprietari (dei metaversi) sovrintendono e

57. Per maggiori informazioni v. il comunicato stampa della Commissione europea *Verso la prossima transizione tecnologica: la Commissione presenta la strategia dell'UE per la leadership sul web 4.0 e i mondi virtuali*.

58. Ma che possono essere qualificate come formazioni sociali ai sensi dell'art. 2 Cost., cfr. DI MAJO 2023.

59. Vedi ora, sul DMSA la ricca analisi di OROFINO 2024, p. 175 ss. Sul DSA vedi la letteratura citata alla nt. 40.

60. SCORZA 2022, p. 15 ss., in proposito, sostiene che «Se si vuole fare in modo che il futuro, nel metaverso, sia migliore del presente e del passato in Internet e se si vuole scongiurare il rischio di tornare a commettere errori che si sono, probabilmente, commessi in passato è necessario far tesoro, almeno ora, delle tante lezioni di Stefano Rodotà: regolamentare per garantire le libertà e i beni comuni anche nella dimensione digitale, farlo fissando principi più che regole di dettaglio, guardare alla dimensione sovranazionale più che a quella nazionale, non dimenticarsi mai di mettere l'uomo al centro, in tutte le sue dimensioni, e non scordare mai che ciascuno di noi deve avere gli stessi diritti – almeno quelli fondamentali – online, in Internet, nella dimensione digitale, nella realtà virtuale, in quella aumentata o nel metaverso che verrà. Lo Stato, probabilmente, deve riappropriarsi di ruoli che, in democrazia, non possono essere “delegati” a soggetti privati: primi tra tutti quelli di dettare le regole della civile convivenza anche nella dimensione digitale e di amministrare la giustizia».

61. La questione delle attribuzioni delle autorità indipendenti in questo ambito è cruciale e può essere approfondito partendo dalla lettura di CALZOLAIO 2024, p. 83 ss.

62. CERRINA FERONI 2023, p. 34, propone «Per il metaverso privatizzato si potrebbe, ad esempio, pensare ad un'amministrazione congiunta di un insieme di organismi, sulla falsariga di ciò che già avviene per Internet (ICANN, W3C, IETF): ognuno di questi enti mostra la propria natura bipolare perché sono società private che orientano le proprie attività in senso pubblicistico».

63. Così POLLICINO 2021, spec. p. 10 ss.

64. Come avverte MONTI 2023, p. 61 ss.

regolano l'interazione dei sudditi (gli utenti) stabilendo le regole e la loro applicazione»⁶⁵.

Come si accennava, per la definizione degli standard tecnici si sta giocando una contesa geopolitica importante fra USA, Cina, Big Tech e Unione europea. Questa contesa ha attualmente attenzione verso il mercato dell'intelligenza artificiale, ma già si sposta, con largo anticipo, nell'ambito della definizione delle norme tecniche del metaverso. Neppure è chiaro se decollerà a livello di mercato questa tecnologia, che già i principali produttori mondiali, come Meta, Microsoft, Epic Games, hanno creato il *Metaverse Standard Forum* per favorire l'interoperabilità in nome di un *Open Metaverse*⁶⁶.

L'obiettivo è anche quello di esplorare il panorama degli standard relativi alla protezione dei diritti digitali. Il *Metaverse Standard Forum* mira prioritariamente, però, a stabilire principi guida che consentano il trasporto, lo scambio, la monetizzazione e l'accesso relativi alle risorse digitali 3D in tutto lo *stack* del metaverso⁶⁷. Si delinea, in questo modo, una pretesa di auto-regolazione che non appare essere una soluzione praticabile in considerazione del livello dei diritti e degli interessi che sono coinvolti. Piuttosto, occorrerà seguire la strada della co-regolazione che, nell'attuale quadro politico-normativo, nell'Ue è demandata alle norme tecniche di armonizzazione, adottate dagli enti di normalizzazione su mandato delle istituzioni europee e sulla base della dichiarazione di interesse pubblico. La tutela e il godimento effettivo delle libertà e dei diritti fondamentali, tuttavia, richiede anche l'intervento dei pubblici poteri. Avendo la disciplina di queste fattispecie natura eminentemente tecnica, le istituzioni dell'Ue non si trovano di fronte ad una sfida facile. Non si può, però, abdicare al compito di provare a dire la propria anche in questi settori al fine di confezionare un diritto a prova di futuro (*future-proof*).

7. Brevi suggestioni conclusive

La politica e il diritto, in definitiva, sono chiamate a prepararsi per tempo ad affrontare la regolazione dei metaversi, partendo dall'enucleazione dei possibili problemi che essi porranno. Il finanziamento,

pubblico e privato, della ricerca in questi ecosistemi e le prospettive di utilizzo della tecnologia dei gemelli digitali dimostrano che la direzione è stata ormai impressa: si cercherà di andare avanti nella costruzione di questi spazi digitali, che determineranno scenari importanti, che non possono essere sottovalutati. Si è mostrato nel corso del presente saggio come anche l'Unione europea sia in prima fila nel finanziamento di queste ricerche e nello sviluppo di questi mondi di realtà aumentata. L'entità del finanziamento è giustificata dalla volontà di evitare nuovamente di ritrovarsi in una situazione di svantaggio competitivo.

Anche le opportunità che queste tecnologie offrono in potenza fanno prevedere che questi ecosistemi si svilupperanno prima o poi, in un modo o nell'altro.

In fondo, essi procedono nella ricerca di sviluppo immaginata dall'uomo e realizzano quell'aspirazione a superare la sua finitezza, che è un anelito umano incessante. Per queste ragioni, la ricerca scientifica andrà nella direzione di travolgere le barriere del possibile e sospingerà ancora più in avanti la trasformazione digitale del mondo, già sin qui travolgente, per poi sperimentare le accresciute possibilità tecnologiche sul corpo umano.

Vecchi e mai sopiti sogni potrebbero essere realizzati nell'universo parallelo digitale, come quello di non smarrire l'elemento più prezioso dell'esistenza umana: i ricordi... dell'esperienza di un momento, delle emozioni o dei sentimenti che si provano in un istante, della loro memoria. I ricordi... che rischiano di svanire perché custoditi nella caducità della mente umana. Se sarà possibile affidarsi a un archivio digitale e riviverli in un altrove, la tentazione di affidarsi ad una simile tecnologia potrà essere irresistibile.

Ancora una volta, la letteratura e la poesia ci aiutano a comprendere la ricerca di senso e le aspirazioni dell'uomo, quali il sogno di invertire la direzione del tempo, di rivivere un momento e di non dimenticarlo o magari di rivivere un'esperienza saggiando un diverso finale. La sperimentazione di un metaverso, insomma, non è sorda rispetto ai sogni e ai bisogni dell'uomo, così come li ha evocati magnificamente Borges in quei versi struggenti

65. CERRINA FERONI 2023, p. 31 s.

66. Cfr. MONTI 2023, p. 81 s.

67. Per ragguagli è possibile consultare il sito di [The Metaverse Standards Forum](https://www.metaversestandardsforum.com/).

di *Elegia di un ricordo impossibile* che ho riportato parzialmente nell'esergo di questo lavoro⁶⁸.

Riferimenti bibliografici

- G. ALPA (2021), *Il diritto di essere se stessi*, La nave di Teseo, 2021
- M. BALCONI, M. IENCA, A. LAVAZZA et al. (2024), *Il caso Neuralink: scienza, etica e le ricadute sociali delle neurotecnologie*, in "Scienzairete", 11 aprile 2024
- M. BALL (2022), *Metaverso. Cosa significa, chi lo controllerà e perché sta rivoluzionando le nostre vite*, Garzanti, 2022
- J. BARRAT (2013), *Our Final Invention. Artificial Intelligence and the End of the Human Era*, Thomas Dunne Books, 2013
- M.E. BUCALO (2022), *I volti della libertà di manifestazione del pensiero nell'era digitale: fra intermediari online, moderazione dei contenuti e regolazione*, Giappichelli, 2022
- BYUNG-CHUL HAN (2023), *Le non cose. Come abbiamo smesso di vivere il reale*, trad. it., Einaudi, 2023
- S. CALZOLAIO (2024), *Autorità indipendenti e di governo della società digitale*, in S. Calzolaio, E. Longo, A. Iannuzzi et al., "La regolazione europea della società digitale", Giappichelli, 2024
- G. CERRINA FERONI (2023), *Il metaverso tra problemi epistemologici, etici e giuridici*, in "MediaLaws", 2023, n. 1
- B.C. CHEONG (2022), *Avatars in the metaverse: potential legal issues and Remedies*, in "International Cybersecurity Law Review", vol. 3, 2022
- C. COLAPIETRO (2022), *Libera manifestazione del pensiero, fake news e privacy, oggi*, in "Dirittifondamentali.it", 2022, n. 2
- R. DE CARIA (2021), *L'impatto della tokenizzazione sui diritti di proprietà*, in "MediaLaws", 2021, n. 3
- L. DI MAJO (2023), *L'art. 2 della Costituzione e il "Metaverso"*, in "MediaLaws", 2023, n. 1
- M. DIETZ, G. PERNUL (2020), *Unleashing the Digital Twin's Potential for ICS Security*, in "IEEE Security & Privacy", vol. 18, 2020, n. 4
- U. ECO (2011), *Apocalittici e integrati. Comunicazioni di massa e teorie della cultura di massa*, Bompiani, 2011
- C. ESPOSITO (1956), *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Giuffrè, 1956
- S. FIORE, F. RESTA (2023), *Il diritto penale nel metaverso*, in P. Stanzione (a cura di), "Il Metaverso. Diritti, Libertà, Antropologia", Edizioni Scientifiche Italiane, 2023
- L. FLORIDI (2022), *Metaverse, a Matter of Experience*, in "Philosophy & Technology", vol. 35, 2022
- G. GIORELLO (2023), *La filosofia di Dylan Dog e altri incubi*, Mimesis, 2023
- A. IANNUZZI (2024), *Le fonti del diritto dell'Unione europea per la disciplina della società digitale*, in S. Calzolaio, E. Longo, A. Iannuzzi et al., "La regolazione europea della società digitale", Giappichelli, 2024

68. Sono debitore della rievocazione degli splendidi versi di Borges al prof. Fabrizio Tigano che, con passione, li ha citati nella sua *Relazione conclusiva* del Convegno *Un diritto virtuale? La regolamentazione giuridica del Metaverso*, Università degli Studi di Messina, 7 luglio 2023, all'interno del quale ho avuto l'opportunità di discutere le mie prime riflessioni sul tema del metaverso, che ho poi sviluppato in questo saggio.

- A. IANNUZZI, F. LAVIOLA (2023), *I diritti fondamentali nella transizione digitale fra libertà e uguaglianza*, in “Diritto costituzionale”, 2023, n. 1
- A. LIGUSTRO, R. TARCHI, G.M. RUOTOLO, G. MARTINICO (a cura di) (2023), *La rappresentazione delle tradizioni giuridiche nella pop culture. Narrazione e percezione del giuridico tra immagini statiche e immagini dinamiche*, Editoriale Scientifica, 2023
- E. LONGO (2024), *La disciplina del “rischio digitale”*, in S. Calzolaio, E. Longo, A. Iannuzzi et al., “La regolazione europea della società digitale”, Giappichelli, 2024
- E. LONGO (2023), *Libertà di informazione e lotta alla disinformazione nel Digital Services Act*, in “Giornale di diritto amministrativo”, 2023, n. 6
- C. MAGNANI (2018), *Libertà di espressione e fake news. Il difficile rapporto tra verità e diritto. Una prospettiva teorica*, in “Costituzionalismo.it”, 2018, n. 3
- R. MANZOCCO (2011), *Dylan Dog. Esistenza, orrore, filosofia*, Mimesis, 2011
- V.A. MARCHESE (2022), *Informazione e conoscenza: «fatto» ed «effetto» nella dimensione olistica dell'infosfera*, in “Nuove autonomie”, 2022, n. 1
- E. MAZZARELLA (2022), *Contro Metaverso. Salvare la presenza*, Mimesis, 2022
- MC KINSEY & COMPANY (2022), *Value creation in the metaverse. The real business of the virtual world*, 2022
- A. MONTI (2023), *Metaverso e convergenza tecnologica: aspetti (geo)politici, giuridici e regolamentari*, in G. Cassano, G. Scorza (a cura di), “Metaverso. Diritti degli utenti – piattaforme digitali – privacy – diritto d'autore – profili penali – blockchain e NFT”, Pacini Giuridica, 2023
- A.C. NAZZARO (2023), *La natura giuridica del metaverso tra Stato, essential facility e giardino privato*, in G. Cassano, G. Scorza (a cura di), “Metaverso. Diritti degli utenti – piattaforme digitali – privacy – diritto d'autore – profili penali – blockchain e NFT”, Pacini Giuridica, 2023
- J. NIDA-RÜMELIN, N. WEIDENFELD (2018), *Umanesimo digitale. Un'etica per l'epoca dell'intelligenza artificiale*, Italian digital edition, FrancoAngeli, 2018
- M. OROFINO (2024), *Il Digital Market Act: una regolazione asimmetrica a cavallo tra diritto della protezione dei dati e diritto antitrust*, in S. Calzolaio, E. Longo, A. Iannuzzi et al., “La regolazione europea della società digitale”, Giappichelli, 2024
- M. OROFINO (2024-A), *Il Digital Service Act tra continuità (solo apparente) ed innovazione*, in S. Calzolaio, E. Longo, A. Iannuzzi et al., “La regolazione europea della società digitale”, Giappichelli, 2024
- M. OROFINO (2022), *La questione del sotto utilizzo dell'intelligenza artificiale in campo sanitario: spunti di rilievo costituzionale*, in “Queste istituzioni”, 2022, n. 4
- A. PACE, M. MANETTI (2006), *Art. 21. La libertà di manifestazione del proprio pensiero*, in “Commentario alla Costituzione”, Zanichelli-Soc. ed. del Foro italiano, 2006
- U. PAGALLO (2022), *Il dovere alla salute. Sul rischio di sottoutilizzo dell'intelligenza artificiale in ambito sanitario*, Mimesis, 2022
- V. PAGNANELLI (2023), *La smart city come ecosistema digitale. Profili di data governance*, in “Dirittifondamentali.it”, 2023, n. 2
- S. PERGAMENO (1963), *Presentazione*, in K. Laumer, “I mondi dell'impero”, La Tribuna, 1963
- O. POLLICINO (2021), *Costituzionalismo, privacy e neurodiritti*, in “MediaLaws”, 2021, n. 2
- A. PRETEROTI (2023), *Ambiente digitale e benessere: la disconnessione come diritto della personalità e strumento di tutela della dignità umana*, in “Ambientediritto”, 2023, n. 3

- G. RESTA (2007), *Identità personale e identità digitale*, in “Il diritto all’informazione e dell’informatica”, 2007, n. 3
- G.M. RICCIO (2023), *Metaverso, logiche proprietarie e poteri privati*, in G. Cassano, G. Scorza (a cura di), “Metaverso. Diritti degli utenti – piattaforme digitali – privacy – diritto d’autore – profili penali – blockchain e NFT”, Pacini Giuridica, 2023
- J. RICHMAN, L. PITMAN, G.S. NANDAKUMAR (2022/2023), *A Gamefied Synthetic Environment for Evaluation of Counter-Disinformation Solutions*, in “Journal of Simulation Engineering”, vol. 3, 2022/2023
- S. RODOTÀ (2006), *La vita e le regole. Tra diritto e non diritto*, Feltrinelli, 2006
- S. RODOTÀ (1990), *Il terribile diritto*, il Mulino, 1990
- U. RUFFOLO (2023), *Piattaforme e content moderation nella dialettica tra libertà di espressione ed autonomia privata*, in “European Journal of Privacy Law & Technologies”, 2023, n. 1
- U. RUFFOLO (2023-A), *Piattaforme e metaverso*, in C. Pinelli, U. Ruffolo, “I diritti nelle piattaforme”, Giappichelli, 2023
- U. RUFFOLO, A. AMIDEI (2019), *Intelligenza Artificiale e diritti della persona: le frontiere del “transumanesimo”*, in “Giurisprudenza Italiana”, 2019, n. 7
- F. SARZANA DI S. IPPOLITO, M.G. PIERRO, I. EPICOCO (2022), *Il diritto del metaverso*, Giappichelli, 2022
- G. SCORZA (2022), *In principio era Internet e lo immaginavamo diverso*, in “Rivista italiana di informatica e diritto”, 2022, n. 1
- W. SHENGLI (2021), *Is Human Digital Twin possible?*, in “Computer Methods and Programs in Biomedicine Update”, vol. 1, 2021
- S. TAGLIAGAMBE (2022), *Metaverso e gemelli digitali. La nuova alleanza tra reti neurali e artificiali*, Mondadori, 2022
- I. ZOPPOLI (2023), *Il diritto alla disconnessione nella prospettiva europea: una road map per le parti sociali*, in “federalismi.it”, 2023, n. 1



BENEDETTO PONTI

Il rapporto tra cybersicurezza e tutela dei dati personali: sinergie, bilanciamenti e parallelismi

Il saggio riflette sulle diverse declinazioni in cui può svolgersi (ed effettivamente si svolge) il rapporto tra cybersecurity e tutela dei dati personali. In particolare, sono individuate tre specifiche declinazioni di questo rapporto, qualificabili rispettivamente in termini di sinergia; di (reciproco) bilanciamento; infine, un rapporto qualificabile in termini di parallelismo. Le diverse sfaccettature del rapporto cybersecurity/tutela dei dati personali non si esauriscono entro questo schema interpretativo. Piuttosto, le tre declinazioni proposte sono individuate quali chiavi di lettura particolarmente interessanti, perché aiutano a cogliere la ricchezza e la densità di tale rapporto. Già in premessa, le chiavi di lettura così proposte tratteggiano i termini di un rapporto niente affatto univoco, e designano una relazione non scontata, né lineare, tra le due grandezze messe a tema. Il saggio si propone anche di dare corpo a questa premessa, corroborando la tesi di un rapporto molto meno diretto e scontato di quanto non si possa ritenere *prima facie*, ciò che implica un livello maggiore di consapevolezza non solo tra gli studiosi e gli addetti ai lavori, ma da parte di tutti gli utenti dei servizi che l'ordinamento appresta a tutela dei dati personali, per un verso, e a tutela della sicurezza cibernetica, per l'altro.

Tutela dei dati personali – Cybersecurity – Sinergia – Bilanciamento – Parallelismo

Synergies, balances, and parallelism between the cybersecurity and personal data protection

In the essay, some declinations of the link between cybersecurity and data protection that may exist – and do exist – are discussed. In particular, three distinct declinations of this relationship are identified, which can be further classified as follows: synergy; (reciprocal) balancing; and finally, a relationship that can be qualified in terms of parallelism. This interpretive scheme does not cover all the aspects of the link between cybersecurity and personal data protection. Rather, the depth and density of this relationship are captured by the three proposed declinations, which are recognized as particularly interesting keys. The terms of a relationship that is by no means unambiguous are outlined in the introduction's keys of interpretation, which also designate a relationship that is neither clear nor linear between the two magnitudes assigned to the topic. The essay aims to provide weight to this assumption by supporting the thesis of a much less clear-cut and direct relationship than one might initially think; this suggests that researchers, practitioners, and all users of the system's services for the protection of cybersecurity and personal data should be aware of this relationship.

Personal data protection – Cybersecurity – Synergy – Balancing – Parallelism

L'Autore è professore associato di Diritto amministrativo presso l'Università degli studi di Perugia

Questo contributo fa parte della sezione monografica *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà*, a cura di Marina Pietrangelo

SOMMARIO: 1. Premessa. – 2. La sinergia tra cybersecurity e tutela dei dati personali. – 3. Il bilanciamento tra cybersecurity e tutela dei dati personali. – 4. Parallelismi tra cybersecurity e tutela dei dati personali.

1. Premessa

Il presente contributo intende evidenziare le diverse declinazioni in cui può svolgersi (ed effettivamente si svolge) il rapporto tra cybersecurity e tutela dei dati personali, da intendersi, entrambe le grandezze, sia in termini di esigenza, di interesse che chiede di essere tutelato, sia con riferimento alla disciplina positiva che è concretamente apprestata a tale fine.

In particolare, vorrei concentrare la mia attenzione su tre specifiche declinazioni di questo rapporto, che potremmo in prima battuta individuare e caratterizzare in questo modo:

- un rapporto qualificabile in termini di sinergia;
- un rapporto qualificabile in termini di (reciproco) bilanciamento;
- un rapporto qualificabile in termini di parallelismo.

Le riflessioni che seguono non hanno la pretesa di esaurire o ricondurre entro questo schema interpretativo tutte le diverse sfaccettature del rapporto cybersecurity/tutela dei dati personali. Piuttosto, chi scrive ritiene che si tratti di chiavi di lettura particolarmente interessanti, perché aiutano a cogliere la ricchezza e la complessità della tematica.

Come si vede, già ad un primissimo sguardo ai “titoli” delle chiavi di lettura proposte, si tratta di declinazioni niente affatto univoche o armoniche tra loro, e che parrebbero designare una relazione non scontata, né lineare, tra le due grandezze. Ciò che mi propongo di fare è anche di dare corpo a questa primissima “impressione”, corroborando la tesi di un rapporto molto meno diretto e scontato di quanto non si possa ritenere *prima facie*, ciò che implica un livello maggiore di consapevolezza non solo tra gli studiosi e gli addetti ai lavori, ma da

parte di tutti gli utenti di questi “servizi” (in definitiva, tutti i cittadini).

2. La sinergia tra cybersecurity e tutela dei dati personali

La prima declinazione del rapporto tra cybersecurity e tutela dei dati personali che metto a tema è la sinergia. Con questo termine, sintetico, mi riferisco alla circostanza per cui, in primo luogo, l'interesse alla sicurezza dell'ambiente, delle risorse, dei servizi che abilitano il ciberspazio ha ambiti, settori di sovrapposizione (e, dunque, di coincidenza) con l'interesse alla tutela dei dati personali. Detto in modo meno rozzo: l'interesse (pubblico) alla sicurezza del ciberspazio muove nella medesima direzione dell'interesse (di ciascun consociato) alla tutela dei dati personali, nella misura in cui la protezione dell'ambiente in cui i dati personali sono destinati ad essere raccolti, conservati, fruiti è funzionale alla tutela del diritto (dei diritti, al plurale) sottesi alla protezione dei dati. Non si tratta, ben inteso, di una coincidenza piena (né sul piano quantitativo, né sul piano qualitativo). E tuttavia, appare evidente che, nella misura in cui la tutela dei dati personali si sostanzia (ad esempio) nel rispetto dei principi sul trattamento di cui all'art. 5 del GDPR, un ambiente sicuro costituisce un fattore che abilita e rafforza il rispetto di questi principi.

Si pensi al principio di *limitazione della finalità del trattamento*: la possibilità di conservare, gestire e trasmettere dati personali in modo sicuro (o, quantomeno, adeguatamente presidiato rispetto a intrusioni) costituisce di per sé un fattore che rende meno probabile l'appropriazione e l'uso dei dati personali per fini diversi da quelli ammessi dalla vigenza del principio di limitazione della finalità. Oppure, si pensi al principio di *minimizzazione*

dei dati: la disponibilità di tecnologie e soluzioni di crittografia (sviluppate e gestite a fini di cybersicurezza) consente più agevolmente di trattare i dati in conformità con questo principio.

O, ancora, si pensi al principio di *integrità e riservatezza*, che costituisce forse la traduzione più aderente delle istanze della cybersecurity nell'ambito della disciplina generale di tutela dei dati personali. E si potrebbe continuare.

Il rapporto di sinergia (in quanto tale) vale anche nel senso opposto, ovvero se osserviamo il rapporto dal punto di vista della cybersecurity. Valga quanto detto adesso con riferimento al principio (un *principio sul trattamento dei dati personali*) di *integrità e riservatezza*. La realizzazione di soluzioni organizzative, procedurali e tecnologiche finalizzate a mitigare il rischio di intrusioni malevole e a contenerne effetti e ricadute, contribuisce largamente a dare seguito e sostanza agli obblighi di sicurezza che gravano sul titolare e sul responsabile del trattamento, per effetto di quanto disposto dall'art. 32 del GDPR.

Se questa sinergia può apparire scontata, con riferimento alle istanze di riservatezza, limitazione, protezione dei dati da intrusioni esterne (la privacy come istanza classica di *esclusione*), va sottolineato che essa trova riscontro anche rispetto all'altro obiettivo della disciplina del GDPR, quello della circolazione dei dati personali. Infatti, un ambiente comunicativo sicuro, perché adeguatamente protetto da minacce esterne, costituisce un fattore indispensabile a favorire la circolazione dei dati (che presuppone il transito degli stessi, quando non il loro stoccaggio in infrastrutture di condivisione).

Dunque, esistono solidi argomenti a dimostrazione di una sinergia (tutt'altro che sorprendente) sul piano dei fini (gli interessi tutelati) e delle discipline positive.

Ma questa sinergia si può riscontrare anche su un piano differente, ovvero quello dell'*approccio* e del *modello di regolazione* adottato a livello di Unione europea. Come è stato efficacemente segnalato in dottrina¹, infatti, se si mettono a confronto la disciplina di tutela dei dati (il GDPR)

e alcune fondamentali discipline in materia di cybersicurezza, quali la direttiva NIS (e NIS2), la PSD2 (la direttiva sui pagamenti digitali) e la direttiva eIDAS (la direttiva sull'identificazione elettronica e i servizi fiduciari), è possibile riscontrare alcune rilevanti *isomorfie* negli approcci regolatori adottati.

Ad esempio, l'*analisi del rischio* come presupposto per la taratura delle misure di protezione da adottare è comune al GDPR come pure alla disciplina PSD2 e alla direttiva NIS2.

Ancora, il principio secondo il quale le esigenze di tutela dei dati personali andrebbero anticipate e inserite nella stessa progettazione dei sistemi (*privacy by design e by default*) si ritrova anche nella disciplina PSD2 e in quella eIDAS².

Il principio per cui ogni *data breach* deve essere opportunamente notificato (*reporting obligation*) è recepito in ciascuna delle discipline richiamate qui sopra, come pure le esigenze di assicurare adeguate procedure di *Business continuity* e di *Disaster recovery*.

Si tratta, come si può notare, di sinergie che si collocano su un piano procedurale e operativo, e che certamente possono aiutare a leggere i diversi *testi regolatori* non come corpi separati (che danno luogo ad una normativa frammentaria), ma piuttosto come sistemi coerenti ed integrati³. Ciò che appare particolarmente utile sul lato delle imprese (come pure delle amministrazioni) che devono sostenere i costi della *compliance*, e che da una prospettiva di questo genere possono trarre vantaggio (e non solo sul piano delle economie di spesa, ma anche su quello della efficacia delle soluzioni così implementate). Ciò è tanto più importante, se si considera che il principio del *risk assessment* – e più in generale, l'approccio regolatorio fondato sulla adeguatezza delle misure adottate e la connessa accountability del titolare (e del responsabile) del trattamento – è tuttora vissuto da una parte significativa del mondo imprenditoriale (con specifico, sebbene non esclusivo, riferimento al settore della media e piccola impresa, e dell'artigianato) come fattore di incertezza, che rende più complesso

1. MANTELERO-VACIAGO 2020; VIGGIANO 2021.

2. Evidenziano l'estensione di tale approccio alla regolamentazione dell'AI, *ex multis*, ANDRAŠKO-MESARČIK-HAMUE-
LÁK 2021.

3. ANGELINI-CICCOTELLI-FRANCHINA et al. 2020.

pianificare ed ammortizzare i costi e implementare le soluzioni adeguate⁴. Un approccio integrato e sistematico, che riguardi i diversi aspetti di *compliance* qui indicati, ne renderebbe più efficiente il recepimento e l'applicazione⁵. Ciò che però sembra richiedere una forte collaborazione, a monte e a valle, anche da parte delle (plurime) autorità di settore coinvolte.

3. Il bilanciamento tra cybersecurity e tutela dei dati personali

Il perseguimento della sicurezza nel ciber spazio può porsi, però, anche come istanza/finalità/interesse idoneo a limitare/ridurre il livello di protezione assicurato ai dati personali. In questo (diverso) schema interpretativo, cioè, il perseguimento dell'una finalità (la sicurezza – anche – nel ciber spazio) entra in relazione di *bilanciamento* con l'esigenza di tutela dei dati personali, tale per cui il peso, l'importanza, la gravità degli interessi sottesi può comportare una *diminutio* del livello di tutela assicurato alla protezione dei dati personali⁶. Sia chiaro, anche la disciplina "ordinaria" di tutela dei dati personali (quella disposta con il GDPR) integra un'operazione di bilanciamento, tra tutela dei dati personali e gli altri interessi in virtù dei quali sono fissati (in quella disciplina) i presupposti, i principi e i diritti connessi al trattamento dei dati. In altre parole, non essendo la tutela dei dati personali un diritto assoluto, ogni normativa che ne disciplina il trattamento comporta in ogni caso una qualche forma di bilanciamento.

Pertanto, qui faccio riferimento ai casi in cui la disciplina positiva di tutela dei dati, qualora il trattamento sia giustificato da esigenze di sicurezza (e, quindi, anche di cybersicurezza), si discosta

da quella generale, proprio in ragione del fatto che – per tali finalità – si giustificato (sono giudicati legittimi) bilanciamenti differenti (rispetto a quelli recepiti nella disciplina ad applicazione generale residuale, quale è quella del GDPR) tra i due interessi in campo.

Come noto, una fondamentale ragione a giustificazione di questo diverso bilanciamento dipende dalla riserva esclusiva in capo agli Stati membri della materia *sicurezza nazionale*, così come sancita nell'art. 4 del TUE⁷, e più in generale dal rispetto delle funzioni essenziali dello Stato, tra le quali certamente le funzioni connesse alla prevenzione, all'indagine e al perseguimento di reati.

Ciò comporta (o contribuisce a determinare) due ordini di conseguenze. In primo luogo, con riferimento alla disciplina del trattamento dei dati personali, quando questa concerne le materie attinenti alla prevenzione, all'indagine e al perseguimento di reati, il rispetto delle funzioni essenziali dello Stato comporta il ricorso ad uno strumento di armonizzazione quale la direttiva, così da lasciare margini significativi allo Stato membro per adattare i principi in materia di tutela dei dati personali alle specificità nazionali. In secondo luogo, con riferimento alla disciplina della cybersecurity, quando questa implica il compimento di funzioni che attengono alla tutela della sicurezza nazionale, ciò la fa ricadere al di fuori dell'ambito coperto dalla relativa disciplina dell'Ue. In questo senso, è significativo quanto ribadito da ultimo dalla direttiva NIS2, all'art. 2, che ne regola l'ambito di applicazione⁸.

Entro queste coordinate, si aprono dunque spazi per un bilanciamento tra i valori in gioco in cui la

4. KAISER 2023; HÄRTING-KAIM-KLAMM-KRONEBERG 2021.

5. NWANKWO-STAUCH-RADOGLU-GRAMMATIKIS et al. 2022.

6. VAN DE POEL 2020; CHRISTEN-GORDIJN-WEBER et al. 2017.

7. «[L'Unione europea] rispetta le funzioni essenziali dello Stato, in particolare le funzioni di salvaguardia dell'integrità territoriale, di mantenimento dell'ordine pubblico e di tutela della sicurezza nazionale. In particolare, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro».

8. Nello specifico, va preso in considerazione il testo dei parr. 6 e 7 dell'art. 2, dove si statuisce che [6] «La presente direttiva lascia impregiudicata la responsabilità degli Stati membri di tutelare la sicurezza nazionale e il loro potere di salvaguardare altre funzioni essenziali dello Stato, tra cui la garanzia dell'integrità territoriale dello Stato e il mantenimento dell'ordine pubblico», e che [7] «La presente direttiva non si applica agli enti della pubblica amministrazione che svolgono le loro attività nei settori della sicurezza nazionale, della pubblica sicurezza o della difesa, del contrasto, comprese la prevenzione, le indagini, l'accertamento e il perseguimento dei reati».

tutela dei dati personali può subire limitazioni entro margini più ampi di quelli contemplati dal GDPR.

Ad esempio quando si tratti di contrastare i *cyber crime*, lo spazio di manovra riconosciuto al legislatore nazionale nel limitare i diritti dell'interessato è più ampio: sia in ragione dello strumento normativo utilizzato (la direttiva), sia in ragione delle specifiche esigenze connesse allo svolgimento delle indagini (oltre che a quelle connesse alla fase più propriamente processuale-penale). Si consideri poi che il novero dei diritti riconosciuti all'interessato è meno esteso di quello sancito nel GDPR, e che sono contemplate ampie ipotesi che ne giustificano la limitazione.

Significativi esempi, quanto alla esplorazione di questi margini di manovra, si trovano nella recente l. n. 137/2023 di conversione del d.l. 105/2023. In particolare, l'art. 2-bis ha introdotto un comma aggiuntivo all'art. 17 del d.l. 14 giugno 2021, n. 82 (istitutivo dell'Agenzia per la cybersicurezza nazionale), in ragione del quale l'Agenzia è tenuta a trasmettere al procuratore nazionale antimafia e antiterrorismo i dati, le notizie e le informazioni rilevanti per l'esercizio delle funzioni di coordinamento delle indagini, di cui all'art. 371-bis del codice di procedura penale.

Di più acuto rilievo (quanto a distanziamento dai criteri ordinari di bilanciamento) è la questione relativa a quella che in dottrina è variamente indicata come *data retention saga*⁹. Come noto, a partire dalla vicenda culminata nella notissima sentenza *Digital Rights Ireland* della Corte di giustizia dell'Ue¹⁰, si è sviluppato nel corso degli anni una sorta di "braccio di ferro" tra gli Stati membri – desiderosi di poter sfruttare in modo pieno le potenzialità di indagine abilitate dalla conservazione integrale dei (meta) dati di traffico delle comunicazioni elettroniche, compresa l'ubicazione (con riferimento alla telefonia mobile) – e la resistenza opposta in particolare dalla giurisprudenza delle corti superiori (CGUE e Corte EDU), tesa piuttosto a ricondurre l'ambito di praticabilità di una simile ingerenza/limitazione del diritto alla tutela dei dati personali entro i parametri coerenti con un giudizio di stretta proporzionalità.

Dal nostro punto di vista (nell'ottica, cioè, del bilanciamento tra esigenze di cybersecurity e di

tutela dei dati personali), questa *querelle* è significativa (ed indicativa) sotto molteplici punti di vista.

In primo luogo, occorre tenere conto della circostanza per cui anche in questo caso viene in rilievo un atto normativo (la direttiva *ePrivacy*) che – per sua natura – apre spazi di attuazione differenziata nei diversi Stati membri, e che pertanto accetta come leciti bilanciamenti anche parzialmente differenziati tra loro. Tanto più che l'“esordio” di tale *querelle* si è svolto con riferimento ad un atto normativo dell'Unione (la direttiva 2006/24/CE, volta proprio ad armonizzare le legislazioni nazionali in materia di *data retention*), cosicché in tale occasione la Corte di giustizia ha fatto diretta applicazione dei principi di cui agli artt. 7, 8 e 52 della Carta dei diritti fondamentali dell'Ue. Sebbene ciò abbia comportato la definizione di un test di proporzionalità sufficientemente stringente (la disciplina di cui trattasi «deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura *de qua* e impongano requisiti minimi in modo che le persone i cui dati sono stati conservati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati»; e quindi: una perimetrazione dei dati da conservare commisurata alla gravità dei reati che si intendono contrastare; la fissazione di criteri oggettivi che permettano di delimitare l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore a fini di prevenzione, di accertamento o di indagini penali; tempi di conservazione proporzionati in relazione alla tipologia di dati e alla loro utilità potenziale in funzione dell'obiettivo perseguito).

Resta però il fatto che la traduzione di un test di tale sorta nei termini di una disciplina positiva lascia spazio a fattispecie applicative anche molto differenziate tra loro (ciò che le vicende successive si sono incaricate di confermare).

Si noti, per altro, che sebbene la *finalità* ultima di tali discipline sia – appunto – l'indagine, l'accertamento e il perseguimento di reati gravi, l'oggetto delle normative si colloca in momento antecedente, e consiste appunto negli obblighi di conservazione posti in capo agli operatori delle comunicazioni elettroniche, funzionali ad abilitare la disponibilità

9. BERGHOLM 2021; GRZELAK 2016.

10. Cause C-293/12 e C-594/12 riunite.

di tali dati per le eventuali finalità di indagine/accertamento/perseguimento dei reati. Si tratta, cioè, di un trattamento posto in essere in prima battuta dagli operatori di mercato, su dati generati nella ordinaria prestazione del servizio. A costo possono, dunque, essere imposti trattamenti *differenziati*, che comportano un diverso (meno intenso) livello di applicazione quantomeno dei principi di “minimizzazione” e di “limitazione della conservazione”.

Nella misura in cui tali limitazioni sono giustificate anche in vista del perseguimento dei c.d. *cybercrime* (e, quindi, anche in funzione di sicurezza cibernetica), ciò dimostra l'operatività di un bilanciamento *differenziato*.

In secondo luogo, nel corso del “braccio di ferro” sulla *data retention*, la giurisprudenza, tanto della Corte di Lussemburgo quanto della Corte di Strasburgo, ha finito per legittimare ipotesi di *bulk data retention*, qualora vengano in considerazione «esigenze di salvaguardia della sicurezza nazionale», ovvero proprio quell'ambito materiale che l'art. 4, par. 2 del TUE riserva alla esclusiva competenza degli Stati membri. Ora, se è vero che a questo riguardo la Corte di giustizia ha chiarito – in premessa – che «una misura nazionale [...] adottata a fini di salvaguardia della sicurezza nazionale non può comportare l'inapplicabilità del diritto dell'Unione e dispensare gli Stati membri dal necessario rispetto di tale diritto», ciò nondimeno «l'interesse primario di tutelare le funzioni essenziali dello Stato e gli interessi fondamentali della società, [interesse che] comprende la prevenzione e la repressione di attività tali da destabilizzare gravemente le strutture costituzionali, politiche, economiche o sociali fondamentali di un paese, e in particolare da minacciare direttamente la società, la popolazione o lo Stato in quanto tale, quali in particolare le attività di terrorismo» – ovvero l'interesse alla sicurezza nazionale – «[è] idoneo a giustificare misure che comportino ingerenze nei diritti fondamentali più gravi di quelle che potrebbero giustificare altri obiettivi»¹¹. In questi casi, cioè, la Corte ammette l'individuazione di un punto di equilibrio in cui il sacrificio dei diritti a tutela

dei dati personali può (legittimamente) risultare più marcato. Tale impianto argomentativo, che distingue la praticabilità di misure di sorveglianza generalizzata in caso di minacce concrete alla sicurezza nazionale (sebbene al netto di alcune garanzie procedurali¹², quali il controllo da parte di una autorità indipendente) e la loro (sostanziale) interdizione nel caso dell'ordinario perseguimento di reati pure “gravi”, è stato ribadito da ultimo, nella sentenza *Commissioner of An Garda Síochána*, del 2022¹³.

Analogo è l'approccio che emerge dalla più recente giurisprudenza della Corte EDU. Nel caso *Big Brother Watch and Others v. the United Kingdom*, deciso dalla Grand Chambre nel maggio del 2021, la Corte era chiamata a valutare la compatibilità con l'art. 8 della Carta CEDU (letto alla luce della Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale) della legislazione inglese allora vigente (il *Regulation of Investigatory Powers Act 2000*, in seguito abrogato e sostituito dall'*Investigatory Powers Act* del 2016). Tale disciplina contemplava misure quali: l'intercettazione massiccia delle comunicazioni (c.d. *bulk interception*) su mandato del governo; lo scambio di dati tra agenzie di intelligence straniere; l'acquisizione dei dati di comunicazione da parte di service providers (*data retention*). La Corte di Strasburgo non esita a riconoscere che tali misure di sorveglianza rivestono «un'importante capacità tecnologica di identificare nuove minacce nel dominio digitale» e che «l'intercettazione massiva è di vitale importanza per gli Stati contraenti nell'individuare le minacce alla loro sicurezza nazionale»¹⁴. Anche sulla scorta di queste considerazioni, la Corte nota come l'art. 8 della Convenzione «non proibisce l'uso di intercettazioni di massa per proteggere la sicurezza nazionale e altri interessi nazionali essenziali contro gravi minacce esterne» e che «gli Stati dispongono di un ampio margine di apprezzamento nel decidere quale tipo di regime di intercettazione sia necessario», margine temperato da alcune garanzie procedurali di

11. Cfr. CGUE, C-511/18 e C-512/18 *La Quadrature du Net*, nonché C-623/17 *Privacy International*.

12. ZALNIERIUTE 2021.

13. Cfr. CGUE, C-140/20.

14. Cfr. ECHR, *Big Brother Watch and Others vs. The United Kingdom* (Applications n. 58170/13, 62322/14 and 24960/15).

base (garanzie la cui assenza ha determinato il giudizio di violazione dell'art. 8, nel caso concreto)¹⁵.

Come si vede, anche in questo caso le finalità connesse alla protezione della sicurezza nazionale, giustificano un punto di equilibrio (che gli Stati possono individuare, in esito all'esercizio del *wide margin of appreciation* loro accordato) nel quale viene giustificato un (ben) più intenso grado di ingerenza sulla protezione dei dati personali rispetto allo standard fissato con il GDPR (o anche nella stessa direttiva 680/2016), in termini convergenti con quanto emerso nella giurisprudenza della CGUE («the two Courts are converging rather than diverging in their recent jurisprudence concerning the data retention saga»¹⁶).

Nella misura in cui la sicurezza nazionale (oggetto di protezione) si configura anche (soprattutto, nei tempi odierni?) come cybersicurezza, emergono molto bene i profili di bilanciamento: il perseguimento della (cyber)sicurezza nazionale è suscettibile di giustificare più forti/rilevanti limitazioni dei diritti degli interessati e degli stessi principi che reggono (ordinariamente) il regime di tutela dei dati personali.

Ma c'è forse qualcosa di più da notare. Le misure mediante le quali si articola la tutela della sicurezza nazionale (anche quelle oggetto di attenzione della giurisprudenza appena richiamata) si configurano, tendenzialmente, come trattamenti automatizzati, che sfruttano le potenzialità tecnologiche, conoscitive, investigative, di intelligence, e che presuppongono un uso dei dati personali *in contraddizione* con i principi sul trattamento lecito (ai sensi, ad esempio, del GDPR o della direttiva 680/2016), quali il principio di limitazione della finalità del trattamento, il principio di minimizzazione dei dati, o quello di limitazione della conservazione. Questa è la ragione per la quale la loro *ammissibilità* richiede un diverso punto di equilibrio (rispetto

a quello codificato nel GDPR e anche nella direttiva 680/2016). Nello stesso tempo, si tratta molto spesso di sviluppare e applicare misure di cybersecurity capaci di muoversi sullo stesso piano di quelle con le quali sono perpetrati gli attacchi alla sicurezza nazionale (alla stregua del proverbio “*a brigante, brigante e mezzo*”, ovvero “*combattere con le armi del nemico*”). E, si noti, non si tratta solo dell'ambito connesso alla materia della difesa (verso nemici “esterni”), declinabile nei termini del *cyberwarfare*, ma anche della *sicurezza interna*¹⁷.

In altre parole, qui ci troviamo di fronte ad un bilanciamento (a sfavore della tutela dei dati personali) applicato perché le esigenze di cybersicurezza siano soddisfatte mediante la predisposizione di mezzi adeguati, perché uguali e contrari a quelli che la mettono in pericolo. Si affacciano, così, (sotto vesti non del tutto inedite) questioni connesse alla tematica classica della *democrazia protetta*: ovvero se e quanto sia possibile non solo *comprimere*, ma addirittura *contraddire* la tutela di diritti fondamentali (quale in questo caso il diritto alla tutela dei dati personali) per fare fronte a minacce esistenziali alla convivenza organizzata¹⁸.

4. Parallelismi tra cybersecurity e tutela dei dati personali

Il terzo rapporto che vorrei evidenziare è declinato in termini di parallelismo, e per illustrarlo vorrei concentrarmi sull'attore pubblico, in particolare le amministrazioni pubbliche. Nella progettazione, realizzazione e implementazione di soluzioni (più o meno) automatizzate che implicano il trattamento di dati personali, così come nel caso di procedure, soluzioni e misure per la cybersecurity, le amministrazioni si trovano nella condizione (necessitata, per una serie plurima di ragioni più o

15. NADDEO 2022; «the real significance of the case lies in endorsing the legality of mass surveillance. Despite the finding of violation, the majority of the GC declared, just as the regular Chamber did in 2018, that mass-surveillance is not, in principle, unlawful and/or disproportionate».

16. TZANOU-KARYDA 2022.

17. Cfr., da ultimo, CGUE, *Valstybės sienos apsaugos tarnyba*, causa C-72/22 PPU, nella quale la Corte osserva che la nozione di sicurezza nazionale «comprende la sicurezza interna di uno Stato membro e la sua sicurezza esterna e, pertanto, il pregiudizio al funzionamento delle istituzioni e dei servizi pubblici essenziali nonché la sopravvivenza della popolazione, come il rischio di perturbazioni gravi dei rapporti internazionali o della coesistenza pacifica dei popoli, o ancora il pregiudizio agli interessi militari, possono ledere la pubblica sicurezza».

18. BROEDERS-CRISTIANO-WEGGEMANS 2023.

meno storicamente determinate) di interagire con il mercato e i suoi attori.

Nel caso del trattamento dei dati personali, perché questo costituisce un risvolto necessitato di qualsiasi soluzione volta a supportare o direttamente concretizzare l'esercizio di funzioni pubbliche mediante il ricorso alle c.d. tecnologie digitali (per usare un termine *riassuntivo*). Questo rapporto è caratterizzato da rilevanti asimmetrie conoscitive (oltre che operative), anche con specifico riferimento agli impatti delle soluzioni progettate/adottate in termini di compatibilità con la disciplina sul trattamento dei dati personali¹⁹.

Non dissimile è il tipo di rapporto che si instaura con i soggetti che forniscono consulenza, soluzioni e prodotti da destinare alla tutela della sicurezza cibernetica delle amministrazioni. Anche qui, il ricorso al mercato è sostanzialmente necessitato, ed è parimenti caratterizzato da rilevanti asimmetrie²⁰. Già questo aspetto indica un evidente parallelismo (per altro in qualche modo implicito nel rapporto di sinergia di cui si è già detto).

Tuttavia, le analogie non si fermano a questa constatazione (di natura prevalentemente *fattuale*). Se si guarda a come tale rapporto (asimmetrico) può essere governato dalla parte “debole”, si scorrono ulteriori similitudini. Un'alternativa possibile è quella di strutturare il rapporto in termini gerarchici, basati sullo schema del *command and control*, nel tentativo di colmare, mediante l'esercizio dell'autorità, una capacità di controllo che l'asimmetria informativa impedirebbe di esercitare. Si tratta di una soluzione che presenta notevoli controindicazioni: tende ad irrigidire le soluzioni così predisposte (condannandole spesso a una scarsa effettività, e comunque a una rapida obsolescenza), impedisce di sfruttare appieno lo stato dell'arte in termini di ricerca e sviluppo e costituisce un incentivo per il partner privato a puntare su commesse quantitativamente importati (sotto il profilo del prezzo) piuttosto che qualitativamente qualificate.

Soprattutto, tende a preservare e consolidare l'asimmetria informativa, rafforzando la condizione di junior partner (sostanziale) in cui l'amministrazione si trova ad operare.

Un approccio alternativo è quello che invece punta a strutturare il rapporto in modo più paritario, su base collaborativa e aperta²¹. Un approccio che può consentire di evitare molte delle controindicazioni prima evidenziate, e avere così soluzioni più flessibili, capaci di incorporare in modo tempestivo le innovazioni, e quindi qualitativamente qualificate). Tuttavia per poter essere perseguito, tale approccio richiede alcune pre-condizioni. In primo luogo, occorre che l'amministrazione disponga di effettivi margini entro i quali sviluppare la collaborazione, ciò che implica una serie di scelte in capo al legislatore, in termini di definizione del framework operativo. Il nuovo Codice dei contratti pare muoversi in questa direzione, come pure coerenti con questa esigenza appaiono le modifiche al Codice privacy in materia di presupposti di liceità per il trattamento dei dati personali per l'esercizio di funzioni pubbliche²². Diversamente, la dottrina maggioritaria segnala come l'architettura nazionale in materia di cybersecurity rifletta un'impostazione metodologica ancora troppo legata al modello dell'*intelligence*, e quindi poco o per nulla caratterizzata in termini di collaborazione e di apertura²³.

Un ulteriore presupposto, indispensabile perché la collaborazione (qualora possibile) non si trasformi in una *colonizzazione* da parte degli attori di mercato²⁴, consiste nel dotare le amministrazioni (il sistema amministrativo) di competenze e capacità utili per potersi confrontare in modo consapevole ed attrezzato con i partner privati. Sotto questo profilo, va evidenziato il ruolo che possono svolgere le università e le altre istituzioni della ricerca pubblica, e vale la pena sottolineare (in questo senso) la *buona pratica* rappresentata dal consorzio Cini²⁵, come esperimento (di successo) non solo nel creare una

19. BHAROSA 2022; TAYLOR 2021.

20. PREVITI 2022.

21. BARONE 2006.

22. PONTI 2023.

23. SERINI 2023; ROSSA 2023; PREVITI 2022; BARONE 2006.

24. MAZZUCCATO-COLLINGTON 2023; TAYLOR 2021.

25. Cfr. il [sito del consorzio](#).

rete, ma anche nel promuovere azioni finalizzate alla maturazione e al trasferimento di conoscenze e competenze cui le amministrazioni possono (eventualmente) attingere, per strutturarsi come player *attivi e attrezzati* del sistema di sicurezza

cibernetica nazionale. Ciò che richiede, evidentemente, investimenti importanti, soprattutto sul fronte del capitale umano. È, questo, un capitolo distinto, e altrettanto importante, che non è possibile nemmeno sfiorare in questa sede.

Riferimenti bibliografici

- J. ANDRAŠKO, M. MESARČÍK, O. HAMUEÁK (2021), *The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework*, in “AI & Society”, vol. 36, 2021, n. 2
- M. ANGELINI, C. CICCOTELLI, L. FRANCHINA et al. (2020), *Italian National Framework for Cybersecurity and Data Protection*, in L. Antunes, M. Naldi, G. Italiano, K. Rannenberg, P. Droghkaris (eds.), “Privacy Technologies and Policy. APF 2020. Lecture Notes in Computer Science”, Springer, vol. 12121
- A. BARONE (2006), *Il diritto del rischio*, Giuffrè, 2006
- N. BHAROSA (2022), *The rise of GovTech: Trojan horse or blessing in disguise? A research agenda*, Government Information Quarterly, vol. 39, 2022, n. 3
- J. BERGHOLM (2021), *The Data Retention Saga Continued—from Tele2 Sverige to Privacy International and La Quadrature du Net*, in “JFT”, vol. 2021, n. 2
- D. BROEDERS, F. CRISTIANO, D. WEGGEMANS (2023), *Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy*, in “Studies in Conflict & Terrorism”, vol. 46, 2023, n. 12
- M. CHRISTEN, B. GORDIJN, K. WEBER et al. (2017), *A Review of Value-Conflicts in Cybersecurity: An assessment based on quantitative and qualitative literature analysis*, in “Orbit, An Online Journal for Responsible Research and Innovation in ICT”, vol. 1, 2017, n. 1, pp. 1-19
- A. GRZELAK (2016), *Data Retention Saga Continues: Decision of the Polish Constitutional Tribunal of 30 July 2014 in Case K 23/11*, in “European Public Law”, vol. 22, 2016, n. 3
- R.C. HÄRTING, R. KAIM, N. KLAMM, J. KRONEBERG (2021), *Impacts of the New General Data Protection Regulation for small-and medium-sized enterprises*, in X.S. Yang, R.S. Sherratt, N. Dey, A. Joshi (eds.), “Proceedings of Fifth International Congress on Information and Communication Technology: ICI-CT 2020”, Springer, vol. 1, 2021, pp. 238-246
- M. MAZZUCCATO, R. COLLINGTON (2023), *The Big Con: How the Consulting Industry Weakens our Businesses, Infantilizes our Governments and Warps our Economies*, Penguin, 2023
- E. KAISER (2023), *The new NIS II Directive and its impact on small and medium enterprises (SMEs): initial considerations*, in “Media laws”, 2023, n. 1
- A. MANTELERO, G. VACIAGO (2022), *Reconciling Data Protection and Cybersecurity: An Operational Approach for Business Sector*, in R. Senigaglia, C. Irti, A. Bernes (eds.), “Privacy and Data Protection in Software Services”, Springer, 2022
- G. NADDEO (2022), *Il difficile bilanciamento tra sicurezza nazionale e tutela dei diritti fondamentali nella “data retention saga” dinanzi alla Corte di giustizia*, in “Freedom, Security & Justice: European Legal Studies”, 2022, n. 2, pp. 188-217
- I. NWANKWO, M. STAUCH, P. RADOGLU-GRAMMATIKIS et al. (2022), *Data Protection and Cybersecurity Certification Activities and Schemes in the Energy Sector*, in “Electronics”, vol. 11, 2022, n. 6, p. 965

- B. PONTI (2023), *Attività amministrativa e trattamento dei dati personali. Gli standard di legalità tra tutela e funzionalità*, FrancoAngeli, 2023
- L. PREVITI (2022), *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, in “federalismi.it”, 2022, n. 25
- S. ROSSA (2023), *Cybersicurezza e pubblica amministrazione*, Editoriale Scientifica, 2023
- F. SERINI (2023), *La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana*, in “Rivista italiana di informatica e diritto”, 2023, n. 2
- L. TAYLOR (2021), *Public Actors Without Public Values: Legitimacy, Domination and the Regulation of the Technology Sector*, in “Philosophy and Technology”, vol. 34, 2021
- M. TZANOU, S. KARYDA (2022), *Privacy International and Quadrature du Net: One Step Forward Two Steps Back in the Data Retention Saga?*, in “European Public Law”, vol. 28, 2022, n. 1
- I. VAN DE POEL (2020), *Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security*, in M. Christen, B. Gordijn, M. Loi (eds.), “The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology”, Springer, vol 21, 2020
- M. VIGGIANO (2021), *Cybersecurity and Data Protection in European Union Policies and Rules: The NIS Directive and the GDPR Synergy*, in G. De Minico, O. Pollicino (eds.), “Virtual Freedoms, Terrorism and the Law”, Routledge, 2021
- M. ZALNIERIUTE (2021), *Procedural Fetishism and Mass Surveillance under the ECHR. Big Brother Watch v. UK*, in “VerfassungsBlog”, 2 June 2021



FEDERICA RESTA

Cybersicurezza e protezione dati: un rapporto ambivalente

Il saggio analizza il rapporto tra protezione dati e cybersicurezza, alla luce dell'evoluzione che lo ha caratterizzato. In particolare, la protezione dati è stata inizialmente e tradizionalmente concepita come parametro di legittimità dell'attività investigativa funzionale alla tutela della cybersecurity. Tuttavia questa declinazione del rapporto tra tali due interessi giuridici, in termini antagonisti, ha lasciato di lì a poco emergere una più interessante sinergia. Si è infatti compreso come, sul terreno del rapporto tra sicurezza (anche cibernetica) e protezione dati si giochi una sfida cruciale per la democrazia: quella di coniugare entrambe per essere più efficaci, non meno liberi.

Sicurezza nazionale – Cybersicurezza – Protezione dati – Protocollo di intesa – Violazione di dati personali

Cybersecurity and data protection: an ambivalent relationship

This paper analyzes the relationship between data protection and cybersecurity in light of its evolution. In particular, data protection was initially and traditionally conceived as a parameter of legitimacy of investigative activity functional to the protection of cybersecurity. However, this declination of the relationship between these two legal interests, in antagonistic terms, allowed a more interesting synergy to emerge shortly thereafter. Indeed, it was understood how, on the ground of the relationship between security (including cybersecurity) and data protection, a crucial challenge for democracy is played out: that of combining both in order to be more effective, not less free.

National security – Cybersecurity – Data protection – Memorandum of understanding – Data breach

L'Autrice è dottoressa di ricerca in Diritto penale. Direttrice del Servizio affari legislativi e istituzionali e del Servizio affari legali, coordinatrice della Segreteria di Presidenza del Garante per la protezione dei dati personali

Questo contributo fa parte della sezione monografica *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà*, a cura di Marina Pietrangelo

SOMMARIO: 1. Il contesto. – 2. Sinergie inattese. – 3. Prospettive.

1. Il contesto

Benché non scontata, anzi spesso fraintesa o ignorata, l'interrelazione tra protezione dati e cybersecurity è tuttavia profonda e consolidata.

Questa sinergia è oggi normativamente espressa dal d.l. 14 giugno 2021, n. 82 istitutivo dell'Agenzia per la cybersicurezza nazionale. Esso sancisce, con dato significativo, le forme della specifica cooperazione dell'Agenzia con il Garante (oltre che la sua consultazione), anche mediante protocolli d'intesa, relativi tra l'altro alle notifiche dei *data breach* (protocollo siglato poi nel febbraio 2022).

Questa previsione richiama, tuttavia, uno schema che ha radici molto più profonde ed è il risultato di un percorso che ha condotto alla sinergia tra questi due interessi a partire, però, da una posizione inizialmente, essenzialmente antagonista. La collaborazione tra Garante e Autorità (prima, essenzialmente, il Dipartimento informazioni per la sicurezza - DIS) a tutela della cybersecurity risale, infatti, al 2013 quando, con la direttiva Monti, si è siglato il primo protocollo d'intesa con il DIS. Esso è stato poi, da allora, rinnovato ed esteso alla comunicazione dei *data breach* e indicato, tanto dall'allora Autorità delegata, on. Marco Minniti, quanto dalla Fundamental Rights Agency dell'Ue, esempio di migliori prassi nella declinazione del rapporto tra privacy e sicurezza nazionale. Rapporto, questo, in costante dinamismo, tanto in ragione del mutamento dei rischi da cui proteggere la «Repubblica e le istituzioni democratiche poste dalla Costituzione a suo fondamento» (come recita la l. 3 agosto 2007, n. 124), quanto a causa della vorticoso evoluzione della tecnica, che amplifica quei rischi e incide, profondamente, sul bilanciamento tra libertà e sicurezza.

È significativo che il primo protocollo nascesse con il fine di introdurre garanzie ulteriori rispetto all'accesso sistematico dei servizi per fini, tra l'altro,

di cybersicurezza, poco prima loro attribuiti dalla “legge D'Alema” (l. 7 agosto 2012, n. 133).

La protezione dei dati rappresentava dunque, in quest'ottica, il limite esterno o, meglio, il parametro di legittimità dell'esercizio di poteri, quali quelli d'intelligence, funzionali alla tutela della cybersicurezza ma, appunto, potenzialmente lesivi della riservatezza. La cybersicurezza rappresentava, dunque, un bene giuridico, metaindividuale, la cui garanzia avrebbe potuto, potenzialmente, ledere la privacy se non correttamente orientata. Di qui il ruolo della protezione dati come condizione di legittimità di attività, pur incisive, a tutela della cybersicurezza nazionale.

Il protocollo veniva siglato in un periodo di grande enfasi, attribuita dalla CGUE, alla proporzionalità nel rapporto tra sicurezza (di cui la sicurezza cibernetica è componente importante) e protezione dati, culminata nella sentenza *Digital Rights* dell'8 aprile 2014 (Cause riunite C293/12 e C594/12) con cui, un anno dopo il protocollo tra Garante e DIS, si è annullata la direttiva 2006/24, appunto per violazione del canone di proporzionalità per quanto riguarda la *data retention*. E l'esigenza di un controllo sul trattamento di dati (anche personali) a fini di sicurezza nazionale, nella sua declinazione di sicurezza cibernetica, è stata soddisfatta perché nel nostro ordinamento, sin dal 1996, la sfera della sicurezza nazionale non è stata sottratta all'ambito applicativo della disciplina di protezione dati, con anzi una previsione innovativa che esclude l'opponibilità del segreto al Garante. Si è trattato di una previsione assai lungimirante, in quanto ha promosso soprattutto la diffusione della cultura della protezione dati in un settore, quale quello della sicurezza nazionale, dominato dalla prevalenza delle istanze pubblicistiche incontrando poi, proprio sul terreno della cybersecurity, significative affinità.

2. Sinergie inattese

Se, dunque, la protezione dati nasceva ed era concepita, nel protocollo d'intesa, come parametro di legittimità dell'attività investigativa funzionale alla tutela della cybersecurity, questa declinazione del rapporto tra tali due interessi giuridici, in termini antagonisti, ha lasciato di lì a poco emergere una più interessante sinergia. Si è infatti compreso come sul terreno del rapporto tra sicurezza (anche cibernetica) e protezione dati si giochi una sfida cruciale per la democrazia: quella di coniugare entrambe per essere più efficaci, non meno liberi.

Proprio il protocollo e l'esigenza, emersa durante la sua attuazione, di proteggere i dati e i sistemi quale presupposto indispensabile per la sicurezza dello spazio cibernetico ci hanno dimostrato, infatti, quanto il rapporto tra protezione dati e cybersecurity viva di sinergie prima – e più ancora – che di antagonismi. La formale sanzione di questa consapevolezza si è avuta nel 2019, quando con un nuovo protocollo tra Garante e DIS si sono normate specifiche procedure per l'informazione del secondo da parte del primo, in ordine a *data breach* che integrino anche violazioni di sicurezza, essendo solo l'inverso normativamente previsto. Da questa previsione emerge la consapevolezza, ormai piena, della sinergia e complementarietà delle due discipline e, quindi, dei due settori di attività.

E questo essenzialmente perché la sicurezza dello spazio cibernetico implica anzitutto, inevitabilmente, la protezione dei dati, dei sistemi, delle infrastrutture di cui esso è composto; dell'ecosistema digitale, in una parola.

Pertanto una normativa, quale quella della protezione dati, che faccia della prevenzione dei dati e dei sistemi dal rischio sociale della vulnerabilità telematica il suo fulcro essenziale non può che promuovere quelle condizioni complessive di protezione indispensabili per la sicurezza cibernetica. La responsabilizzazione dei titolari, promossa dal Regolamento UE 2016/679, rispetto al rischio "sociale" derivante da sistemi informatici permeabili rappresenta, in questo senso, una risorsa preziosa (anche di tipo reputazionale) e, non a caso, valorizzata anche dalla normativa in materia di cybersecurity. Per altro verso, la garanzia, promossa dalla disciplina di cybersicurezza, di condizioni complessive di sicurezza, resilienza, affidabilità dell'ecosistema digitale anche, come recita il d.l. 82/21, in funzione della sicurezza nazionale, non

può che agevolare la riservatezza dei flussi informativi cui mira la disciplina di protezione dati. E l'evoluzione delle due discipline, con lo snodo del 2016 per la direttiva NIS 1 (2016/1148), ora sostituita dalla NIS 2 (2022/2555) e il Regolamento UE 2016/679 – Regolamento generale sulla protezione dei dati, ha valorizzato ancor più questa sinergia, come sottolineato dal Presidente del Garante.

Il legislatore europeo ha anzi instaurato una significativa simmetria tra protezione dati e sicurezza cibernetica, particolarmente evidente in alcuni istituti che accomunano il Regolamento e la direttiva NIS 1, la NIS 2, fino poi al *Cybersecurity Act* (2019/881).

Così l'obbligo, per gli Stati membri, di provvedere affinché operatori di servizi essenziali e fornitori di servizi digitali adottino – pena rilevanti sanzioni – misure di sicurezza adeguate ai rischi del settore era stato mutuato dalla disciplina di protezione dati sin dalla direttiva 95/46 e ulteriormente rafforzato con il Regolamento, secondo un approccio fondato sul rischio cui corrisponde l'adozione di misure adeguate.

Quest'affinità percorre anche il *Cyber Resilience Act* (approvato definitivamente il 12 marzo 2024), rispetto al quale, ad esempio, il parere n. 23 del 2022 del Garante europeo per la protezione dei dati suggeriva di includere i criteri di sicurezza previsti in materia di protezione dati all'interno dei requisiti essenziali di sicurezza per l'immissione nel mercato dei prodotti digitali, includendovi anche le garanzie di *privacy by design*. E questo, anche considerando che il Regolamento generale sulla protezione dei dati non si rivolge ai produttori.

La stessa idea – promossa dal Regolamento generale sulla protezione dei dati – della garanzia *by design* – da realizzarsi cioè sin dalla progettazione dei dispositivi e dei sistemi – non è affatto estranea alla "filosofia" delle due direttive NIS e, poi, ancor più, al *Cyber Resilience Act*. Essa, infatti, concepisce la sicurezza informatica come un fattore che sul piano logico e cronologico non può considerarsi eventuale o successivo, ma deve "nascere" contestualmente al trattamento.

Di qui l'approccio preventivo di entrambi i plessi normativi (con obblighi di gestione del rischio estesi, con la direttiva NIS 2, a tutta la *supply chain*) e la responsabilizzazione – comune a entrambi – degli operatori, per i quali la protezione dei dati

e dei sistemi diviene un vero e proprio fattore di accountability e di competitività.

Affine è anche il ruolo svolto dalle certificazioni nel complessivo approccio preventivo, comune ad entrambi i plessi normativi.

Comune a entrambe è poi l'istituto della notificazione di eventi pregiudizievoli, volta a consentire – pena l'irrogazione di elevate sanzioni – l'intervento delle autorità rispettivamente competenti secondo tempistiche stringenti (con anche la previsione di un "preallarme" nel caso degli incidenti di sicurezza). Anche in tal caso la disciplina di cybersecurity riprendeva un istituto, quale quello della notificazione di *data breach*, consolidato nel settore della protezione dati in quanto, essendo stato introdotto settorialmente dalla direttiva 2009/136, è stato poi esteso dal Regolamento generale sulla protezione dati alla generalità dei titolari.

L'interrelazione tra cybersecurity e protezione dati è talmente forte rispetto all'istituto dei *breach* (che spesso integrano tanto violazioni di sicurezza quanto di protezione dati), come appunto detto, da aver fondato l'esigenza di specifici protocolli d'intesa tra Garante, appunto e autorità competenti in materia di cybersicurezza (dopo il d.l. 82/21, l'Autorità per la cybersicurezza nazionale).

Anche il recente disegno di legge sulla cybersecurity, approvato definitivamente il 19 giugno 2024, prevede una significativa sinergia tra le competenze del Garante per la protezione dei dati e quelle dell'Autorità per la cybersicurezza nazionale rispetto alla crittografia, per la cui disciplina si prevede infatti una reciproca consultazione dei due organismi.

3. Prospettive

Tale complementarietà tra protezione dati e sicurezza cibernetica non è, del resto, casuale, se si pensa, come sottolineato dal Presidente del Garante, che la protezione dati è stata inizialmente concepita, sin dai tempi della direttiva 95/46, come un bene giuridico che ciascuno Stato membro avrebbe dovuto tutelare adeguatamente per poter entrare nell'area Schengen, in quanto presupposto per la sicurezza dell'area stessa.

Questa concezione in termini di sinergia, tutt'altro che di opposizione, era ovviamente quantomai lungimirante, instaurando un parallelismo significativo tra libertà di circolazione delle persone (e quindi dei dati personali) e sicurezza delle

informazioni, a beneficio dei singoli e della collettività, oltre che della democrazia.

E se questa sinergia riguarda essenzialmente gli attori istituzionali, la sfida da vincere oggi è realizzare questa cooperazione anche con i vari soggetti, anche privati, coinvolti nella complessa filiera del digitale: non si può pensare di rendere sicura la supply chain in assenza di una reale responsabilizzazione di ogni suo anello, come peraltro ben dispone la direttiva NIS 2. Se per la cybersecurity si è parlato, a ragione, di bene comune (o pubblico secondo le declinazioni) perché appunto non rivale e non escludibile, ciò comporta anche il necessario coinvolgimento, nell'opera di messa in sicurezza dell'ecosistema digitale, degli operatori a vario titolo incidenti su esso; la cybersecurity esige responsabilità condivise, seppure asimmetriche.

La stessa proposta di *Cyber Resilience Act* valorizza il partenariato pubblico privato in funzione di resilienza, sovranità/indipendenza tecnologica, leadership intesa anche come contrasto della parcellizzazione dei centri di responsabilità e rafforzamento della governance in una dimensione olistica di gestione del rischio.

Inutile dire quanto ciò sia centrale in un contesto di guerra per la prima volta davvero ibrida, di traslazione delle ostilità in quello che è stato definito il sesto dominio, quando la frontiera digitale diviene bersaglio elettivo di atti ostili se e in quanto più vulnerabile di quella tradizionale. L'inclusione del 5G tra le tecnologie soggette al golden power dimostra la consapevolezza di quanto le neotecnologie siano centrali e strategiche anche in termini di difesa.

Bisogna dunque estendere la sinergia sperimentata già tra Garante e Autorità a tutela della cybersecurity a tutti gli attori, pubblici e privati, coinvolti a vario titolo dai processi d'innovazione, tanto più con l'IA, promuovendo partenariati pubblico-privati, enti di ricerca, settori diversi. La complessità del digitale esige un'adeguata articolazione nella governance, tanto più alla luce di innovazioni come il metaverso, l'*Internet of Things* e l'IA. È questa una delle più importanti sfide che si delineano nel prossimo futuro.



LORENZO NANNIPIERI

Cybersicurezza e appalti. Interventi legislativi e prime criticità

Negli ultimi anni sta emergendo, nell'ordinamento italiano, la relazione tra contratti pubblici e cybersicurezza. Con una serie di interventi normativi succedutisi a breve distanza di tempo, il legislatore ha innestato con vigore la sicurezza informatica nell'ambito della disciplina degli appalti. Il presente contributo evidenzia i tratti salienti della normativa vigente, sottolineandone alcuni punti critici, in attesa che l'intero quadro regolatorio venga recepito dalle amministrazioni e interpretato dalla giurisprudenza.

Cybersicurezza – Appalti – Contratti pubblici

Cybersecurity and procurement. Legislative interventions and initial critical issues

Recently, the relationship between public contracts and cybersecurity has been emerging at a regulatory level. With a series of regulatory interventions that followed one another in a short space of time, the Italian legislator has vigorously included cybersecurity in the context of procurement regulations. This contribution highlights the salient features of the current legislation, highlighting some critical points, waiting for the entire regulatory framework to be implemented by the administrations and interpreted by administrative courts case-law.

Cybersecurity – Public procurement – Public contracts

L'Autore è ricercatore presso l'Istituto di Informatica Giuridica e Sistemi Giudiziari del CNR

Questo contributo fa parte della sezione monografica *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà*, a cura di Marina Pietrangelo

SOMMARIO: 1. Le norme applicabili. – 2. Il ruolo centrale (e talvolta ripetitivo) dell'art. 14 della l. n. 90/2024. – 3. Una (parziale) conclusione.

1. Le norme applicabili

Negli ultimi anni, il tema della cybersicurezza ha acquisito un deciso “slancio” nella produzione normativa, disancorandosi da disamine proprie di ambiti extra-giuridici della conoscenza per approdare nel campo delle politiche pubbliche e, in definitiva, del diritto sostanziale, tanto da introdurre un nuovo tema di dibattito, legato all'esistenza di un “diritto alla cybersicurezza” di matrice individuale o collettiva¹.

La cybersicurezza è diventata un tema cruciale nel diritto contemporaneo, poiché il crescente utilizzo di tecnologie digitali espone individui, aziende e Stati a nuovi rischi e minacce informatiche. La protezione delle informazioni e dei sistemi digitali è ormai una necessità, non solo dal punto di vista tecnico, ma anche giuridico. In un contesto globalizzato, dove le normative nazionali sono spesso insufficienti a garantire una protezione adeguata, emergono nuove sfide legate alla governance della cybersicurezza e all'impatto non solo sui diritti dei cittadini ma anche sull'organizzazione

amministrativa e sulla gestione dei servizi pubblici, finendo per intersecare in modo tangibile l'organizzazione delle Pubbliche Amministrazioni.

La P.A., come noto, è destinataria di stringenti obblighi derivanti, da ultimo, dall'attuazione della Direttiva NIS 2², come recepita dal d.lgs. 4 settembre 2024, n. 138³.

Se, da un lato, la NIS 2 apporta una cospicua serie di obblighi alla generalità delle Pubbliche Amministrazioni, dall'altro, ulteriori fonti normative si sono susseguite e stratificate in merito ad ambiti *particolari* dell'attività amministrativa.

Tra questi rientra il settore in cui le Amministrazioni condensano i propri poteri di scelta dei contraenti per l'esecuzione di lavori, servizi e forniture, e cioè gli appalti pubblici⁴.

Il tema è attualmente oggetto di alcune disposizioni normative, tutte di recentissima produzione e contenute, sostanzialmente, in tre fonti tra loro eterogenee: il codice dei contratti pubblici (d.lgs. n. 36/2023), la l.n. 90/2024 e il decreto di recepimento della Direttiva NIS 2 (d.lgs. n. 138/2024).

1. Cfr., senza pretesa di esaustività, CAMISA-SIMONCINI 2024; LONGO 2024; MORONI 2024; DI CORINTO 2022; SIMONCINI 2021; DE VERGOTTINI 2019, p. 67 ss.

2. In conformità all'art. 7, comma 1, della Direttiva NIS 2, ciascuno Stato membro è tenuto a elaborare una strategia nazionale per la cybersicurezza, la quale deve definire non solo obiettivi strategici ma anche le risorse e gli strumenti normativi e operativi necessari per il loro perseguimento. Lo scopo è garantire e mantenere un livello elevato e costante di protezione contro le minacce cibernetiche, mediante l'adozione di misure strategiche e normative idonee a rispondere alle sfide in evoluzione. La citata direttiva pone in capo agli Stati membri l'obbligo di adottare misure strategiche riguardanti, tra l'altro, «l'inclusione e la definizione di requisiti concernenti la cybersicurezza per i prodotti e i servizi TIC negli appalti pubblici, compresi i requisiti relativi alla certificazione della cybersicurezza, alla cifratura e l'utilizzo di prodotti di cybersicurezza open source» (art. 7, comma 2, lett. b).

3. Cfr. CASAROSA 2024; PIETRANGELO 2024; BUFFA 2023.

4. COCCHI 2024; ROSSA 2024; sia altresì consentito rinviare a NANNIPIERI 2024.

L'art. 19 del codice dei contratti pubblici contiene quello che è stato definito in dottrina come il «manifesto di politica di cybersicurezza»⁵, enunciando, rispettivamente, al comma 1, il principio secondo cui le stazioni appaltanti «garantiscono l'esercizio dei diritti di cittadinanza digitale e operano secondo i principi di neutralità tecnologica, di trasparenza, nonché di protezione dei dati personali e di sicurezza informatica»; al comma 5, che gli stessi soggetti «adottano misure tecniche e organizzative a presidio della sicurezza informatica e della protezione dei dati personali. Le stazioni appaltanti e gli enti concedenti assicurano la formazione del personale addetto, garantendone il costante aggiornamento».

L'art. 14 del d.lgs. 28 giugno 2024, n. 90 (Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici) rappresenta la disposizione centrale in materia di cybersicurezza e appalti. La disposizione, che si connota per una formulazione particolarmente articolata, prevede che:

«1. Con decreto del Presidente del Consiglio dei ministri, da adottare entro centoventi giorni dalla data di entrata in vigore della presente legge, su proposta dell'Agenzia per la cybersicurezza nazionale, previo parere del Comitato interministeriale per la sicurezza della Repubblica (...), sono individuati, per specifiche categorie tecnologiche di beni e servizi informatici, gli elementi essenziali di cybersicurezza che i soggetti di cui all'articolo 2, comma 2, del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, tengono in considerazione nelle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici nonché i casi in cui, per la tutela della sicurezza nazionale, devono essere previsti criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO) o di Paesi terzi individuati con il decreto di cui al presente comma tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione. Ai fini del presente articolo, si intende per "elementi essenziali di cybersicurezza" l'insieme di criteri e regole tecniche la conformità ai quali, da parte di

beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela di cui al primo periodo.

2. Nei casi individuati ai sensi del comma 1, le stazioni appaltanti, comprese le centrali di committenza:

a) possono esercitare la facoltà di cui agli articoli 107, comma 2, e 108, comma 10, del codice dei contratti pubblici, di cui al decreto legislativo 31 marzo 2023, n. 36, se accertano che l'offerta non tiene in considerazione gli elementi essenziali di cybersicurezza individuati con il decreto di cui al comma 1;

b) tengono sempre in considerazione gli elementi essenziali di cybersicurezza di cui al comma 1 nella valutazione dell'elemento qualitativo, ai fini dell'individuazione del miglior rapporto qualità/prezzo per l'aggiudicazione;

c) nel caso in cui sia utilizzato il criterio del minor prezzo, ai sensi dell'articolo 108, comma 3, del codice di cui al decreto legislativo n. 36 del 2023, inseriscono gli elementi di cybersicurezza di cui al comma 1 del presente articolo tra i requisiti minimi dell'offerta;

d) nel caso in cui sia utilizzato il criterio dell'offerta economicamente più vantaggiosa, ai sensi dell'articolo 108, comma 4, del codice di cui al decreto legislativo n. 36 del 2023, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del migliore rapporto qualità/prezzo, stabiliscono un tetto massimo per il punteggio economico entro il limite del 10 per cento;

e) prevedono criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti alla NATO o di Paesi terzi individuati con il decreto di cui al comma 1 tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione, al fine di tutelare la sicurezza nazionale e di conseguire l'autonomia tecnologica e strategica nell'ambito della cybersicurezza.

3. Le disposizioni di cui al comma 1 si applicano anche ai soggetti privati non compresi tra quelli di cui all'articolo 2, comma 2, del codice di cui al decreto legislativo 7 marzo 2005, n. 82, e inseriti nell'elencazione di cui all'articolo 1, comma 2-bis, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

5. ROSSA 2024, p. 342.

4. Resta fermo quanto stabilito dall'articolo 1 del citato decreto-legge n. 105 del 2019 per i casi ivi previsti di approvvigionamento di beni, sistemi e servizi di information and communication technology destinati ad essere impiegati nelle reti e nei sistemi informativi nonché per l'espletamento dei servizi informatici di cui alla lettera b) del comma 2 del medesimo articolo 1».

L'art. 108, comma 4, del codice dei contratti pubblici, poi, prevede che

«nelle attività di approvvigionamento di beni e servizi informatici, le stazioni appaltanti, incluse le centrali di committenza, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del miglior rapporto qualità prezzo per l'aggiudicazione, tengono sempre in considerazione gli elementi di cybersicurezza, attribuendovi specifico e peculiare rilievo nei casi in cui il contesto di impiego è connesso alla tutela degli interessi nazionali strategici».

Merita attenzione, *a latere*, l'art. 26 del codice che, nella formulazione attuale, prevede che

«1. I requisiti tecnici delle piattaforme di approvvigionamento digitale, nonché la conformità di dette piattaforme a quanto disposto dall'articolo 22, comma 2, sono stabilite dall'AGID di intesa con l'ANAC e la Presidenza del Consiglio dei ministri, Dipartimento per la trasformazione digitale, entro sessanta giorni dalla data di entrata in vigore del codice.

2. Con il medesimo provvedimento di cui al comma 1 sono stabilite le modalità per la certificazione delle piattaforme di approvvigionamento digitale.

3. La certificazione delle piattaforme di approvvigionamento digitale, rilasciata dall'AGID, consente l'integrazione con i servizi della Banca dati nazionale dei contratti pubblici. L'ANAC cura e gestisce il registro delle piattaforme certificate».

Tale ultima disposizione è oggetto dell'intervento correttivo attualmente all'esame delle Camere⁶, secondo cui l'AgID dovrebbe stabilire non i «requisiti tecnici delle piattaforme digitali di e-procurement», bensì «le modalità di certificazione dei medesimi requisiti tecnici delle citate piattaforme di approvvigionamento e la loro conformità all'ecosistema nazionale di approvvigionamento digitale».

Queste modalità di certificazione, peraltro, dovrebbero essere stabilite dall'AgID d'intesa non più solo con l'ANAC e la Presidenza del Consiglio dei ministri – Dipartimento per la trasformazione digitale, ma anche con l'Agenzia per la cybersicurezza nazionale, in ragione della sua specifica competenza.

Da ultimo, deve rilevarsi che il d.lgs. 4 settembre 2024, n. 138, nel recepire la Direttiva NIS 2, ha previsto, all'art. 24, comma 2, che le misure cui i c.d. “soggetti NIS” (essenziali e importanti) sono chiamati ad adottare, dovranno necessariamente contemplare misure finalizzate a garantire la «sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi».

2. Il ruolo centrale (e talvolta ripetitivo) dell'art. 14 della l. n. 90/2024

La disposizione centrale relativa all'impatto della cybersicurezza nelle procedure di appalto è costituita dall'art. 14 della l. 90/2024.

Preliminarmente, non può non evidenziarsi come la collocazione sistematica della disciplina desti qualche perplessità, in relazione all'esistenza di una fonte organica di regolamentazione della materia, e cioè il codice dei contratti pubblici.

L'art. 14 è finalizzato ad introdurre una «disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici».

Come precisato nella relazione tecnica allegata al disegno di legge, le norme introdotte dalla l. n. 90/2024 si prefiggono l'obiettivo primario di garantire un rafforzamento delle tutele connesse alle esigenze di cybersicurezza. Questo aspetto riveste particolare rilievo in tutte le ipotesi in cui le procedure di approvvigionamento delle Pubbliche Amministrazioni siano funzionalmente legate alla salvaguardia degli interessi strategici nazionali.

È utile ricordare, come già premesso, che il codice dei contratti pubblici impone alle stazioni appaltanti un obbligo generale di considerare gli *elementi* di cybersicurezza. Tale obbligo assume carattere più stringente – ancorché con contorni

6. A.G. n. 226, “Schema di decreto legislativo recante disposizioni integrative e correttive al codice dei contratti pubblici di cui al decreto legislativo 31 marzo 2023 n. 36”; si rinvia, sul punto, al parere favorevole espresso in sede consultiva da Cons. Stato, Comm. Spec., 2 dicembre 2024, n. 1463/2024.

applicativi non del tutto definiti – in tutti quei casi in cui l'appalto riguardi attività incidenti sugli interessi nazionali strategici.

Sul piano oggettivo, l'art. 14 rinvia a due nozioni di difficile delimitazione: quella degli "interessi nazionali strategici" e quella degli "elementi essenziali di cybersicurezza".

La prima ("interessi nazionali strategici") costituisce altresì un requisito di applicabilità della disposizione, nel senso che la stessa, *a contrariis*, parrebbe inapplicabile agli appalti per l'approvvigionamento di beni e servizi informatici in "contesti" diversi da quelli connessi alla tutela, appunto, degli "interessi nazionali strategici".

In tale ultimo ambito, peraltro, la disposizione intercetta la formulazione dell'art. 108, comma 4, d.lgs. 36/2023, già richiamato nelle premesse.

Problematica, però, è l'individuazione di un concetto positivo di "interesse nazionale strategico", ricorrente sia nell'articolo in esame che nel codice.

Sul punto, l'art. 14 della l. n. 90/2024 parrebbe operare un rimando implicito agli artt. 5 e 7 del d.l. 82/2021 che, nell'istituire l'ACN, le affida il ruolo di tutore degli «interessi nazionali nel campo della cybersicurezza», affidando all'Agenzia anche la funzione di promotrice delle azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche riguardo «a prodotti e processi informatici di

rilevanza strategica a tutela degli interessi nazionali nel settore».

L'ordinamento contiene effettivamente disposizioni riferibili, a vario titolo, al carattere "strategico" di determinate "attività" (si vedano, ad esempio, i diffusi richiami contenuti nel d.l. 21/2012, "norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni", nonché nel d.l. 187/2022, "misure urgenti a tutela dell'interesse nazionale nei settori produttivi strategici").

Quello che risulta tuttora mancante, però, è una nozione ordinamentale "organica" di "interesse nazionale strategico" che consenta di delimitare con sufficiente precisione l'ambito applicativo sia dell'articolo in commento che del già vigente art. 108 del codice dei contratti pubblici⁷.

Alcuni commentatori, sul punto, hanno rilevato che la nozione di "interessi nazionali strategici" di cui all'art. 14 della l. n. 90/2024 rappresenti una categoria più ampia rispetto ad altre simili, come quella di "sicurezza nazionale" di cui al d.l. 105/2019, nell'ambito della disciplina del Perimetro di sicurezza nazionale cibernetica⁸.

Allo stato attuale, specialmente in considerazione della grande proliferazione di norme di rango primario e regolamentare, sembra esistere

7. Per una definizione di "funzione essenziale dello Stato", parzialmente affine a quella di "interesse nazionale strategico", si rinvia all'art. 2, comma 1, lett. a), d.P.C.M. 131/2020, secondo cui «un soggetto esercita una funzione essenziale dello Stato, di seguito funzione essenziale, laddove l'ordinamento gli attribuisca compiti rivolti ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti».

8. Così ROSSA 2024, p. 354, il quale evidenzia, sul punto, che tale interpretazione "estensiva" della categoria degli interessi nazionali strategici «pare essere confermata dall'art. 10 co. 1 e co. 3 del citato d.d.l. 16 febbraio 2024 A.C. 1717. Nell'elencare coloro i quali sono tenuti a rispettare gli elementi essenziali di cybersecurity nelle procedure di aggiudicazione di beni informatici, la norma menziona due distinte tipologie di soggetti: quelli indicati dall'art. 2, co. 2, d.lgs. n. 82/2005 (ovvero: Pubbliche Amministrazioni, gestori di servizi pubblici e società a controllo pubblico) e quelli privati previsti dall'art. 1, co. 2-bis, d.l. n. 105/2019 ma non ricompresi dal menzionato art. 2, co. 2, d.lgs. n. 82/2005 (vale a dire: soggetti privati ricompresi nel perimetro di sicurezza nazionale cibernetica (PSNC), aventi sede nel territorio nazionale, dai quali dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale). Prevedendo anche soggetti ulteriori rispetto a quelli ricompresi nel perimetro di sicurezza nazionale cibernetica, il d.d.l. pare delineare un concetto di "interesse nazionale strategico" differente e maggiormente esteso rispetto a quello di "sicurezza nazionale" previsto dalla disciplina del PSNC».

effettivamente un problema tassonomico/definitorio⁹, la cui risoluzione appare urgente sia per garantire efficacia al diritto positivo che per ridurre al massimo i rischi di contenzioso amministrativo in un settore – quello degli appalti – già di per sé particolarmente critico, tanto da essere destinatario, ormai “storicamente”, di specifiche misure normative deflative.

La seconda nozione che delimita l'ambito oggettivo di applicazione dell'art. 14 è quella di “elementi essenziali di cybersicurezza”, dizione ricorrente, anch'essa, nel già citato art. 108, comma 4, del d.lgs. 36/2023¹⁰.

È utile ricordare, come già premesso, che il codice dei contratti pubblici impone alle stazioni appaltanti un obbligo generale di considerare gli *elementi* di cybersicurezza. Tale obbligo assume carattere più stringente – ancorché con contorni applicativi non del tutto definiti – in tutti quei casi in cui l'appalto riguardi attività incidenti sugli interessi strategici nazionali.

Rispetto a quest'ultima disposizione, l'art. 14 ha il pregio di sperimentare un'*actio finium regundorum*, fornendo una definizione normativa di “elementi essenziali di cybersicurezza”, da intendersi come «l'insieme di criteri e regole tecniche la conformità ai quali, da parte di beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela di cui al primo periodo».

Il tentativo in esame merita una valutazione positiva, in quanto si configura come un intervento idoneo a colmare una lacuna normativa derivante dalla formulazione, per certi aspetti carente, dell'art. 108, comma 4, del d.lgs. n. 36/2023. Tale disposizione, infatti, nel fare riferimento agli

“elementi di cybersicurezza”, non ha provveduto a fornire una delimitazione chiara e univoca del relativo ambito definitorio, lasciando margini di incertezza interpretativa che possono incidere negativamente sull'applicazione pratica della norma stessa.

La definizione introdotta dall'art. 14, pertanto, sembra rivolta a integrare tale mancanza mediante una precisazione normativa che contribuisca a determinare, con maggiore chiarezza, il perimetro concettuale e operativo degli elementi di cybersicurezza richiamati nella disposizione. In tal modo, si punta non solo a garantire un'applicazione più uniforme e coerente della disciplina, ma anche a soddisfare le esigenze di certezza del diritto richieste dagli operatori del settore, i quali necessitano di riferimenti normativi chiari per conformarsi alle previsioni legislative e regolamentari.

Rimane ferma, però, l'esigenza di distinguere gli “elementi essenziali di cybersicurezza” dagli “elementi di cybersicurezza” di cui all'art. 108, comma 4, del codice, atteso che il requisito dell'*essenzialità* (presente nell'art. 14 in commento ma non nell'art. 108, comma 4, del codice) appare, a propria volta, un concetto sfuggente e di difficile delimitazione¹¹.

Dal punto di vista soggettivo, l'art. 14 della l. 90/2024 richiama «i soggetti di cui all'articolo 2, comma 2, del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 8» individuando, dunque, quali destinatari:

1. le Amministrazioni dello Stato, istituti e scuole di ogni ordine e grado, istituzioni educative, aziende ed amministrazioni dello Stato ad ordinamento autonomo, Regioni, Province, Comuni, Comunità montane e loro consorzi e associazioni, istituzioni universitarie, Istituti autonomi case popolari, Camere di commercio,

9. Come evidenziato da COCCHI 2024, p. 196, il concetto di “interessi nazionali strategici” sconta «una non indifferente genericità, tanto che già dalle prime applicazioni la centrale di Committenza Consip ha escluso la rilevanza strategica di alcune procedure, onde escludere l'applicabilità del comma 4 dell'art. 108 del nuovo Codice».

10. Di “peccato originale delle regole sulla sicurezza nazionale” parla MONTI 2023, secondo cui «una criticità che balza immediatamente all'occhio è il ricorso alla categoria “interessi nazionali strategici” come elemento discriminante per attivare l'obbligo di valutazione separata della componente “sicurezza” dell'offerta, invece di fare riferimento a categorie pur non esattamente definite ma già presenti nell'ordinamento come quelle che appartengono al perimetro nazionale di sicurezza cibernetica, alle infrastrutture critiche e al golden power. Questa criticità affligge sia la scrittura del bando, sia la definizione e la documentazione dei criteri di aggiudicazione».

11. Secondo COCCHI 2024, p. 200, la definizione normativa è «ancora insufficiente per fornire alle stazioni appaltanti indicazioni sufficientemente chiare», in attesa di un intervento chiarificatore che potrebbe giungere con il d.P.C.M. attuativo dell'art. 14 della l. 90/2024.

industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, amministrazioni, aziende ed enti del Servizio sanitario nazionale, ARAN, altre Agenzie di cui al decreto legislativo 30 luglio 1999, n. 300;

2. le autorità di sistema portuale;
3. le autorità amministrative indipendenti di garanzia, vigilanza e regolazione;
4. i gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse;
5. le società a controllo pubblico, con esclusione delle società quotate.

Questo elenco di destinatari delle disposizioni in materia di appalti pubblici contenute nell'art. 14 appare decisamente ampio.

Come osservato in sede istruttoria, l'ambito di applicazione della disposizione avrebbe potuto essere meglio definito, in quanto il rinvio *per relationem* all'art. 2, comma 2, d.lgs. 82/2005 parrebbe condurre ad una generalizzata efficacia applicativa della disposizione stessa anche a soggetti che non svolgono attività di approvvigionamento di beni e servizi informatici legati alla tutela di interessi nazionali strategici¹².

Si pensi, ad esempio, alla generalità delle società a controllo pubblico, ovvero agli istituti di istruzione ovvero, ancora, alla generalità indiscriminata degli enti locali.

Il terzo comma dell'art. 14 allarga ulteriormente la portata applicativa della norma, ricomprendendo anche i soggetti privati inclusi nel Perimetro di sicurezza nazionale cibernetica di cui all'art. 1 d.l. 105/2019.

Si tratta degli operatori privati aventi una sede nel territorio nazionale «da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare

un pregiudizio per la sicurezza nazionale» (art. 1, comma 1, d.l. 105/2019).

L'elencazione di tali soggetti è contenuta in un atto amministrativo della Presidenza del Consiglio dei Ministri su proposta del Comitato interministeriale per la Cybersicurezza, sottratto al diritto di accesso e agli obblighi di pubblicazione (art. 1, comma 2-bis, d.l. 105/2019).

Il secondo comma dell'art. 14 in commento prevede che «nei casi individuati ai sensi del comma 1, le stazioni appaltanti, comprese le centrali di committenza (...) possono esercitare la facoltà di cui agli articoli 107, comma 2, e 108, comma 10, del codice dei contratti pubblici, di cui al decreto legislativo 31 marzo 2023, n. 36, se accertano che l'offerta non tiene in considerazione gli elementi essenziali di cybersicurezza individuati con il decreto di cui al comma 1».

In buona sostanza, nelle ipotesi in cui la stazione appaltante ritenga non rispettati i requisiti previsti dall'emanando d.P.C.M. in tema di «elementi essenziali di cybersicurezza» nella predisposizione dell'offerta, diverrebbe possibile procedere con la non aggiudicazione dell'appalto stesso all'offerente che abbia presentato l'offerta economicamente più vantaggiosa.

La disposizione sembra conferire alla cybersicurezza una rilevanza centrale nell'ambito dei contratti pubblici, indipendentemente al criterio di aggiudicazione previsto dalla stazione appaltante (offerta economicamente più vantaggiosa o prezzo più basso).

Tanto appare «forte» tale indirizzo normativo, che l'art. 14 contiene alcune disposizioni normative che parrebbero ridondanti rispetto alla (già vigente) disciplina del codice dei contratti pubblici.

In particolare, lo stesso comma 2 dell'art. 14, al punto b), dispone che le stazioni appaltanti «tengono sempre in considerazione gli elementi essenziali di cybersicurezza di cui al comma 1 nella valutazione dell'elemento qualitativo, ai fini dell'individuazione del miglior rapporto qualità/prezzo per l'aggiudicazione».

12. Come evidenziato dall'ANCI in sede di istruttoria parlamentare, «se da un lato il riferimento all'art. 2 comma 2 del CAD lascia intendere che si applichi a tutti i Comuni e loro società controllate, dall'altro si parla di approvvigionamento di beni e servizi informatici legati alla tutela degli interessi nazionali strategici. Nel caso di interesse, i Comuni, in base alla classificazione operata dalla stessa ACN, sono gestori di informazioni e dati ordinari, ad eccezione di Roma Capitale e Milano». Cfr. il [contributo scritto dell'ANCI](#).

Tale disposizione non sembra molto dissimile (apparendo, anzi, ridondante) rispetto a quanto già previsto dall'art. 108 del codice, nella parte in cui si prevede che «le stazioni appaltanti, incluse le centrali di committenza, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del miglior rapporto qualità prezzo per l'aggiudicazione, tengono sempre in considerazione gli elementi di cybersicurezza, attribuendovi specifico e peculiare rilievo nei casi in cui il contesto di impiego è connesso alla tutela degli interessi nazionali strategici».

Ancora, secondo la successiva lettera d), le stazioni appaltanti, «nel caso in cui sia utilizzato il criterio dell'offerta economicamente più vantaggiosa, ai sensi dell'articolo 108, comma 4, del codice di cui al decreto legislativo n. 36 del 2023, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del migliore rapporto qualità/prezzo, stabiliscono un tetto massimo per il punteggio economico entro il limite del 10 per cento». Senonché l'art. 108, comma 4, del codice, già specifica che «quando i beni e servizi informatici oggetto di appalto sono impiegati in un contesto connesso alla tutela degli interessi nazionali strategici, la stazione appaltante stabilisce un tetto massimo per il punteggio economico entro il limite del 10 per cento».

Alla lettera c) del secondo comma dell'art. 14, invece, il legislatore ha introdotto l'obbligo di inserimento degli elementi di cybersicurezza tra i requisiti minimi dell'offerta, anche nel caso di utilizzo del criterio del minor prezzo, di cui all'art. 108, comma 3, del codice.

In buona sostanza, l'art. 14 parrebbe determinare un effetto estensivo delle prescrizioni dell'art. 108, quarto comma (riferite agli appalti affidati con il criterio dell'offerta economicamente più vantaggiosa) anche ai casi di utilizzo del criterio del minor prezzo.

Anche in questo caso, però, l'intervento legislativo avrebbe trovato una migliore collocazione sistematica direttamente nel codice.

Inoltre, la concreta applicazione della disposizione normativa contenuta nell'art. 108 del codice, nella sua portata prescrittiva ed esecutiva, appare suscettibile di generare un significativo incremento del contenzioso dinanzi alla giustizia amministrativa. Tale rischio risulta amplificato dalla natura non adeguatamente circoscritta della nozione

di «interessi nazionali strategici», che si configura come un concetto giuridico indeterminato, suscettibile di interpretazioni divergenti anche in sede giurisdizionale.

Ulteriore fonte di criticità è rappresentata dalla complessità degli obblighi cui gli operatori economici sarebbero tenuti ad adempiere in materia di cybersicurezza, con particolare riferimento alla distinzione tra elementi «essenziali» e «non essenziali» di sicurezza cibernetica, il cui confine normativo risulta ancora incerto. A ciò si aggiunga che l'ampiezza della discrezionalità riconosciuta alle Stazioni appaltanti nella valutazione delle offerte per quanto attiene al rispetto degli adempimenti prescritti in ambito cyber potrebbe determinare difformità applicative.

3. Una (parziale) conclusione

Il tema della cybersicurezza nell'ambito degli appalti è in fase di «emersione».

Allo stato attuale, è possibile, però, raggiungere una conclusione solo parziale, dovendosi prendere atto di quanto appaia decisa la spinta del legislatore verso l'implementazione delle misure di sicurezza cibernetica nell'ambito dei contratti pubblici. Tanto che la produzione normativa in materia, per quanto non sempre ordinata, non nasconde – ed anzi esplicita – la volontà di raccordare la sicurezza informatica con altri principi cardine dell'azione amministrativa in materia di *procurement*, quali i principi di neutralità tecnologica, trasparenza e protezione dei dati personali.

Non è possibile, ad oggi, valutare l'effettiva portata applicativa di questo nuovo quadro regolatorio, risultante dalla «triangolazione» tra il codice dei contratti pubblici, il decreto attuativo della Direttiva NIS 2 e la l. n. 90/2024, in assenza di specifiche prassi amministrative e, soprattutto, senza la possibilità (ad ora) di capire *se e quando* la giurisprudenza amministrativa avrà la possibilità di intervenire a fronte di aggiudicazioni di contratti pubblici in cui la valutazione degli aspetti connessi alla cybersicurezza possa avere avuto una rilevanza decisiva o preponderante.

Riferimenti bibliografici

- M. BUFFA (2023), *La direttiva NIS II cybersecurity in Europa: tra innovazione, formazione e diritto vivente*, in “Democrazia e Diritti Sociali”, 2023, n. 1
- F. CAMISA, A. SIMONCINI (2024), *Il fattore umano e la regolazione della cybersecurity*, in “Mondo Digitale”, 2024, n. 103
- F. CASAROSA (2024), *L'armonizzazione degli obblighi di notifica: il DDL Cybersicurezza verso la NIS 2*, in “Rivista italiana di informatica e diritto”, 2024, n. 1
- T. COCCHI (2024), *La Cybersicurezza nel prisma del diritto dei contratti pubblici: un tentativo di ricostruzione delle regole del gioco tra requisiti di partecipazione, criteri di aggiudicazione ed esigenze di certezza*, in “Munus”, 2024, n. 1
- G. DE VERGOTTINI (2019), *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, in “Rivista AIC”, 2019, n. 4
- A. DI CORINTO (2022), *Data commons: privacy e cybersecurity sono diritti umani fondamentali*, in “Rivista italiana di informatica e diritto”, 2022, n. 1
- E. LONGO (2024), *Il diritto costituzionale e la cybersicurezza. Analisi di un volto nuovo del potere*, in “Rassegna Parlamentare”, 2024, n. 2
- A. MONTI (2023), *L'impatto del nuovo Codice degli appalti sulla cybersecurity della Pa*, in “Formiche.net”, 13 aprile 2023
- L. MORONI (2024), *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, in “federalismi.it”, 2024, n. 14
- L. NANNIPIERI (2024), *Cybersicurezza e appalti pubblici: verso un nuovo (e incerto) quadro regolatorio*, in “Rivista italiana di informatica e diritto”, 2024, n. 1
- M. PIETRANGELO (2024), *Per un modello nazionale di cybersicurezza cooperativa e resilienza collaborativa*, in “Rivista italiana di informatica e diritto”, 2024, n. 1
- S. ROSSA (2024), *Appalti pubblici e cybersecurity, fra (maggiore) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*, in “CERIDAP”, 2024, n. 2
- A. SIMONCINI (2021), *Sistema delle fonti e nuove tecnologie. Le ragioni di una ricerca di diritto costituzionale, tra forma di stato e forma di governo*, in “Osservatorio sulle fonti”, 2021, n. 2



FEDERICO NICCOLÒ RICOTTA

Vulnerability disclosure e penetration testing: profili giuridici rilevanti per l'adozione di una politica nazionale conforme alla Direttiva NIS 2

Il contributo analizza le principali questioni giuridiche connesse all'adozione di politiche di cosiddetta *vulnerability disclosure*, espressione con la quale si designa il processo di comunicazione e correzione delle falle nella sicurezza, e i cosiddetti *penetration test*, attività che simula un attacco informatico proprio allo scopo di far emergere le vulnerabilità nella sicurezza. Da un lato, l'interesse pubblico alla sicurezza cibernetica delinea gli oneri dei soggetti pubblici e privati per correggere, ma soprattutto comunicare le vulnerabilità; dall'altro, l'attività di *penetration test*, laddove sia condotta da soggetti diversi dal titolare del sistema, può costituire reato. Da qui, la ricerca di un possibile bilanciamento, che consenta di salvaguardare la sicurezza cibernetica attraverso la repressione penale degli illeciti commessi in quest'ambito, senza però disincentivare l'emersione di situazioni di vulnerabilità, attraverso la segnalazione da parte di quanti sono stati in grado di testare le fragilità dei sistemi informatici. Tale disamina sarà effettuata pure in prospettiva comparata, tenendo conto della soluzione adottata nella Repubblica Francese.

Crimini informatici – Vulnerabilità – Test di sicurezza – Recepimento NIS 2 – Notizia di reato

Vulnerability disclosure and penetration testing: relevant legal profiles for the adoption of a national policy compliant with the NIS 2 Directive

The paper examines the main legal issues related to the adoption of so-called vulnerability disclosure policies, a term that refers to the process of communicating and addressing security flaws, and penetration testing, an activity that simulates a cyberattack with the specific aim of identifying security vulnerabilities. On one hand, the public interest in cybersecurity outlines the responsibilities of public and private entities to not only address but also communicate vulnerabilities; on the other hand, penetration testing, when conducted by individuals other than the system owner, may constitute a criminal offense. This raises the need to find a possible balance that ensures cybersecurity by penalizing unlawful acts in this area, while avoiding discouragement of the reporting of vulnerabilities by those capable of testing the weaknesses of IT systems. This analysis will also include a comparative perspective, taking into account the solution adopted in the French Republic.

Vulnerability disclosure – Penetration testing – NIS 2 – Hacking – Cyber crimes

L'Autore è dottore di ricerca in Procedura penale e assegnista di ricerca in SEcurity and RIghts in the CyberSpace

Questo contributo fa parte della sezione monografica *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà*, a cura di Marina Pietrangelo

SOMMARIO: 1. Introduzione. – 2. Vulnerabilità e *penetration testing*. – 3. I modelli di *vulnerability disclosure*. – 4. CSIRT e politiche di *coordinated vulnerability disclosure*. – 5. Esenzione di responsabilità dell'attività di *penetration testing*. – 6. La politica di CVD adottata nella Repubblica Francese. – 7. Una scriminante procedurale come possibile porto sicuro per i *penetration tester*? – 8. Anonimato delle segnalazioni e comunicazione della notizia di reato e controllo giudiziario sulle condotte autorizzate. – 9. L'anonimato attraverso l'assenza di comunicazione della notizia di reato. – 10. L'anonimato e le garanzie funzionali. – 11. Conclusioni.

1. Introduzione

L'art. 12 della direttiva NIS 2 prevede l'istituzione di una banca dati europea delle vulnerabilità e, soprattutto, prescrive che, in sede di attuazione nazionale, ciascuno Stato membro adotti una propria politica di regolazione delle modalità di rilevamento delle vulnerabilità dei sistemi informatici.

L'adozione d'una politica di *coordinated vulnerability disclosure*, d'ora in poi CVD, conforme ai desiderata della NIS 2 richiede tre adempimenti strutturali, che saranno analizzati nei paragrafi che seguono: la tipologia di *vulnerability disclosure* che definisca il coordinamento tra i soggetti pubblici e privati interessati dalla procedura ed una duplice garanzia per il tester di sicurezza in termini di esenzione da responsabilità e anonimato della segnalazione.

Come si vedrà, le disposizioni legislative di recepimento, adottate in Italia con il d.lgs. 4 settembre 2024 n. 138, hanno regolamentato soltanto l'organo competente a ricevere e gestire le segnalazioni di vulnerabilità, lasciando ancora da definire i profili relativi alla responsabilità e all'anonimato del segnalante.

2. Vulnerabilità e *penetration testing*

Nella loro dimensione massimalista le politiche di CVD si riassumono nelle tre fasi della emersione, comunicazione e correzione di una vulnerabilità.

La vulnerabilità è un insieme di condizioni che consente la violazione della sicurezza o della riservatezza di un sistema. È sostanzialmente una

falla nella sicurezza informatica che, in quanto tale, si presta ad essere sfruttata per scopi malevoli. In quanto rischio strutturale per la sicurezza, se la vulnerabilità viene scoperta, dovrebbe essere comunicata tempestivamente: anzitutto allo sviluppatore del sistema informatico, affinché venga corretta; in secondo luogo, se la legge lo prevede, anche all'autorità pubblica di settore, se la vulnerabilità ha l'attitudine a compromettere interessi ultra-individuali rilevanti sul piano pubblicitario. Questo può accadere, i.e., in relazione ai sistemi che rientrano nel perimetro di sicurezza cibernetica e che, come tali, sono sottoposti alla vigilanza dell'Agenzia per la cybersicurezza nazionale. Nella comunicazione circa l'esistenza della vulnerabilità è l'attività di *disclosure*: in Italia, per esempio, è il CSIRT (acronimo di *Computer Security Incident Response Team*) ad essere destinatario delle informative sui rischi dei sistemi e delle infrastrutture digitali.

Le vulnerabilità emergono solitamente attraverso l'esecuzione dei cd. *penetration test*, quali pratiche comuni nella sicurezza informatica che, simulando un atto hacker, hanno lo scopo di identificare le debolezze nei sistemi informatici. I test possono essere condotti da soggetti interni alla società che sviluppa il sistema, oppure da soggetti esterni, pubblici o privati, che operano con o senza la consapevolezza ed il consenso delle entità proprietarie dei sistemi, per esempio nel corso dei cd. *Bug Bounty Programs*, vale a dire quando un'organizzazione offre ricompense (spesso economiche)

a chi riesce a scoprire e segnalare vulnerabilità nei loro sistemi, applicazioni o servizi¹.

Per questo, come si vedrà, queste attività, così come gli strumenti utilizzati per i test, possono costituire la condotta materiale di un reato o rilevare in sede civile. Del resto, e qui risiede l'ulteriore profilo di interesse per la regolazione pubblica, ragioni economiche, reputazionali o legate a segreti industriali possono disincentivare i privati, ma anche le amministrazioni, a non far emergere pubblicamente le vulnerabilità dei propri prodotti e, quindi, a non consentire che siano i terzi a condurre i *penetration test*.

3. I modelli di *vulnerability disclosure*

La prassi cibernetica conosce tre modelli di *vulnerability disclosure*², che differiscono tra loro in ragione del diverso grado di intervento e coordinamento tra chi con la propria attività fa emergere le vulnerabilità e le segnala, chi sviluppa o è proprietario dei sistemi vulnerabili e l'eventuale autorità pubblica deputata all'esercizio di una funzione di cybersicurezza³.

Il tratto comune delle *vulnerability disclosure* è l'essere un processo tramite il quale vengono rivelate le vulnerabilità di sicurezza in software o sistemi a chi può risolverle, tendenzialmente prima che queste informazioni diventino note al pubblico generale. Questo processo, quindi, consente a venditori, sviluppatori, gestori e ricercatori IT che rilevano una vulnerabilità di cooperare per trovare soluzioni che riducano il rischio associato alle vulnerabilità pubbliche; cioè, un ricercatore (chi trova) che scopre un difetto in un sistema, informa lo sviluppatore (venditori, fornitori) del sistema riguardo al difetto e alle possibili correzioni. Questo consente allo sviluppatore di prendere misure di mitigazione (patch, monitoraggio del traffico, blocco) per eliminare o ridurre il rischio che la vulnerabilità sia utilizzata da un attaccante.

A partire da questa matrice comune le soluzioni, come anticipato, si dividono tra divulgazione pubblica o *full disclosure*, divulgazione responsabile o

responsibile disclosure e divulgazione coordinata o *coordinated disclosure*.

Nella *full disclosure* le informazioni sulla vulnerabilità vengono pubblicate apertamente e in modo che chiunque possa accedervi; nella *responsible disclosure* le informazioni sulla vulnerabilità vengono condivise privatamente con il fornitore del software o hardware interessato, dando loro il tempo di risolvere il problema prima che la vulnerabilità sia resa pubblica, anche attraverso una timeline concordata tra chi ha scoperto la vulnerabilità e il fornitore per la correzione e la successiva divulgazione pubblica; infine la *coordinated disclosure*, che consiste in un processo strutturato attraverso il quale le vulnerabilità sono segnalate al fabbricante o al fornitore dei prodotti TIC o dei servizi TIC potenzialmente vulnerabili, in modo tale da consentire loro di diagnosticarle ed eliminarle prima che informazioni dettagliate in merito siano divulgate a terzi o al pubblico⁴. Secondo questo modello, quello prescelto dalla stessa direttiva NIS 2, la divulgazione delle informazioni sulla vulnerabilità viene gestita in collaborazione tra ricercatori, fornitori e talvolta anche organizzazioni di terze parti, come i CERT (Computer Emergency Response Team) o i CSIRT.

4. CSIRT e politiche di *coordinated vulnerability disclosure*

Il primo pilastro delle politiche di CVD riguarda certamente la gestione delle segnalazioni e tutto ciò che ne consegue in termini di comunicazioni e correzioni.

Appare evidente che la stessa NIS 2 prediliga il modello di gestione coordinata della disclosure e lo affida alle competenze del CSIRT nazionale e, per quanto non espressamente conferito, all'Agenzia per la cybersicurezza nazionale dal quale il CSIRT dipende.

Il legislatore nazionale si è quindi mosso conformemente al modello indicato dalla NIS 2 e, all'art. 16 del Decreto Legislativo 4 settembre 2024 n.138 di recepimento della direttiva europea, ha designato il

1. V. FIORINELLI-ZUCCA 2024.

2. *Ivi*, p. 5 ss. e NIS COOPERATION GROUP 2023 e ENISA 2016.

3. V. in generale ROSSA 2023; URSI 2023, p. 7 ss.; PUPILLO-FERREIRA-VARISCO 2018; HOUSEHOLDER-WASSER-MANN-MANION-KING 2017.

4. Cfr. Considerando n. 58 della direttiva NIS 2.

CSIRT Italia quale coordinatore della divulgazione coordinata delle vulnerabilità e intermediario tra il soggetto segnalante e quello produttore o fornitore del servizio ICT potenzialmente vulnerabile.

Si è quindi scelto di impostare l'implementazione delle politiche assecondando un criterio di accentramento delle diverse funzioni connesse alle CVD in un unico polo operativo deputato, da un lato, a gestire le segnalazioni in via riservata, assicurando l'anonimato del segnalante, dall'altro, a procedere agli adempimenti necessari per comunicare e avviare la correzione della vulnerabilità tra i vari soggetti interessati dalla procedura.

La scelta del modello non è casuale ma coerente con la necessità di soddisfare i diversi interessi sottesi al modello di gestione coordinata: in primo luogo, assicurare la tutela dello sviluppatore e della pubblica sicurezza cibernetica, affinché l'esistenza di una potenziale falla nella sicurezza dei sistemi non venga resa indiscriminatamente nota al pubblico, con il rischio di essere malevolmente sfruttata nelle more che venga risolta, ma che essa venga corretta in linea con le prescrizioni tecnico-operative impartite dall'Agenzia stessa; inoltre, garantire la tutela del soggetto segnalante sotto il duplice profilo dell'esenzione da responsabilità e della garanzia dell'anonimato.

5. Esenzione di responsabilità dell'attività di *penetration testing*

Il secondo pilastro delle politiche interne di *coordinated vulnerability disclosure* è quello che insiste

sui profili di responsabilità penale e civile di chi effettua i *penetration test*.

La tutela di chi opera legittimamente nel campo della sicurezza cibernetica risulta ancora uno dei profili da normare, probabilmente il più rilevante, per un'implementazione conforme alle indicazioni della NIS 2 che, a mente del considerando n. 60, richiede agli Stati membri di adottare misure atte a proteggere i ricercatori dalla loro potenziale esposizione alla responsabilità penale e civile per le attività svolte.

Il rapporto tra crimini informatici e le *vulnerability disclosure* si presenta piuttosto complesso e non nuovo, soprattutto se si guarda alle esperienze pilota avvenute oltreoceano⁵.

Dal punto di vista del diritto nazionale italiano, la variabilità dell'esposizione a responsabilità penale è essenzialmente legata all'effettiva offensività della condotta di *penetration test* che, conseguentemente, traccia il limite oltre al quale l'hacking per finalità di ricerca e di sicurezza può causare danni ai sistemi considerati accettabili per l'ordinamento.

Nel diritto penale italiano la criminalizzazione delle condotte riconducibili all'attività di *penetration testing* opera essenzialmente su tre livelli: quello delle attività prodromiche, che riguardano essenzialmente l'uso di software cd. *dual use*, vale a dire programmi che consentono la violazione dei sistemi⁶; quello dell'esecuzione vera e propria dei test attraverso attacchi simulati potenzialmente riconducibili all'accesso abusivo a sistema

5. Il problema è stato affrontato negli USA. A livello federale la principale legge è il *Computer Fraud and Abuse Act* (CFAA) del 1986 (il cd. statuto federale "anti-hacking"), che ha configurato l'accesso non autorizzato a un sistema informatico, in particolare a un sistema governativo o commerciale quale l'atto di «accedere consapevolmente a un computer senza autorizzazione o eccedere le condizioni dell'accesso autorizzato». Il problema si è conseguentemente concentrato sulla vaghezza del significato "eccedere le condizioni dell'accesso autorizzato", con il rischio di criminalizzare un ampio novero di condotte, ulteriori a quelle di *penetration testing*, laddove si pongano in contrasto con i termini di licenza o delle condizioni di uso del software. È intervenuta sul punto la Corte suprema degli USA, stabilendo e.g. in *Van Buren v. United States* che in materia di accesso abusivo e condizioni di autorizzazione non rilevano le regole EULA (*End User License Agreement*)).

6. Le principali fattispecie sono quelle considerate all'art. 615-*quater* c.p. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici; all'art. 615-*quinquies* c.p. Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico; all'art. 617-*quinquies* c.p., Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche; all'art. 171-*bis*, co. 1, legge diritto di autore; all'art. 171-*ter*, co. 1, lett f), legge diritto di autore; all'art. 171-*ter*, co. 1, lett. f-*bis*), legge diritto di autore; v. per un approfondimento CADOPPI-CANESTRATI-MANNA-PAPA 2023 ed in particolare SALVADORI 2017.

informativo, all'intercettazione di sistema informatico o al danneggiamento dei sistemi⁷.

La criminalizzazione si fonda essenzialmente sulla rilevanza della natura abusiva della condotta di chi opera su sistemi informatici o ricorre a determinati strumenti, ricomprendendo tutte quelle attività intenzionalmente nocive e soprattutto condotte in assenza del consenso dell'avente diritto⁸. Per altro, sul piano strettamente penalistico, con l'art. 615 ter c.p. il legislatore ha inteso sanzionare l'accesso abusivo ad un sistema informatico o telematico, o la permanenza non autorizzata in esso, in quanto tali. Non assume infatti alcuna rilevanza, ai fini della consumazione dell'illecito, né l'effettiva presa di conoscenza di dati o informazioni, né la natura di questi ultimi né, soprattutto, le motivazioni che hanno mosso il soggetto agente⁹.

6. La politica di CVD adottata nella Repubblica Francese

Come anticipato, adottare una politica di CVD che sia in linea con le aspettative della direttiva NIS 2 richiede la previsione di un'area di esenzione da responsabilità del *penetration tester* per tutte quelle attività che, sebbene siano necessarie a far emergere una vulnerabilità, possono in condotte materiali di rilevanza penale.

Una soluzione interessante, ma come si vedrà inattuabile nel nostro ordinamento, è quella adottata nel 2016 in Francia, dove un tester può far

emergere una sospetta vulnerabilità all'*Agence nationale de la sécurité des systèmes d'information* (ANSSI) e giovare della disciplina dell'Art. 47 della Loi per une République Numérique che esenta da responsabilità penale il ricercatore che ha effettuato in buona fede le operazioni di *penetration testing*. Effettuata la comunicazione, è compito dell'ANSSI proteggere l'anonimato del segnalante e delle informazioni relative alla scoperta della vulnerabilità.

Il funzionamento dell'esimente francese si caratterizza per una spiccata interconnessione tra le attività giudiziarie e quelle amministrative dell'ANSSI, che invero assume un ruolo di primissimo piano.

Anzitutto, il meccanismo di tutela opera attraverso la facoltà di non esercitare l'azione penale: il menzionato Art. 47, attraverso la modifica dell'art. L 2321-4 *Code de la défense*¹⁰, consente al pubblico ministero di non perseguire penalmente¹¹ il tester laddove ricorrano congiuntamente due condizioni: il tester che segnala una vulnerabilità deve aver agito in buona fede e la vulnerabilità deve essere segnalata esclusivamente all'ANSSI che, s'è detto, si occupa anche di garantire le condizioni di anonimato.

A sua volta, la valutazione di buona fede effettuata dal Pubblico Ministero, quindi sulla meritevolezza dell'azione penale a fronte di condotte potenzialmente criminose ma utili per la sicurezza

7. Le principali fattispecie sono art. 615-ter c.p., Accesso abusivo a Sistema informatico; art. 617-bis c.p., Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche; artt. 635-ter e 635-quinquies c.p., Danneggiamento di dati e sistemi pubblici; artt. 635-bis e 635-quater, Danneggiamento di dati e sistemi privati; v. nota precedente per i riferimenti bibliografici.

8. Vedi per tutti FIORINELLI-ZUCCA 2024, p. 8 ss. e FLOR 2020-A, p. 165 ss. e FLOR 2020.

9. Cfr. FLOR 2020-A, p. 165 ss.

10. Tradotta, la disposizione stabilisce che ai fini della sicurezza dei sistemi informatici, non si applica l'obbligo previsto dall'articolo 40 del codice di procedura penale nei confronti di chi trasmette in buona fede all'autorità unica nazionale per la sicurezza dei sistemi informativi informazioni sull'esistenza di una vulnerabilità riguardante la sicurezza di un sistema di trattamento automatizzato dei dati. L'autorità preserva la riservatezza dell'identità della persona all'origine della trasmissione nonché delle condizioni in cui questa è stata effettuata. L'autorità può compiere le operazioni tecniche strettamente necessarie per caratterizzare il rischio o la minaccia di cui al primo comma del presente articolo, al fine di allertare l'host, l'operatore o il responsabile del sistema informativo.

11. La deroga contenuta nell'art. 2321-4 *Code de la défense* agisce sull'art. 40 del Codice di procedura penale francese in materia di esercizio dell'azione penale e obbligo di denuncia del pubblico ufficiale: il pubblico ministero riceve le denunce e valuta il seguito da dare loro conformemente alle disposizioni dell'articolo 40-1 (codice di procedura penale).

cibernetica, poggia sulle regolamentazioni fornite dall'ANSSI: il grado della buona fede richiesto per beneficiare dell'esenzione penale è essenzialmente il grado di aderenza del tester alle stesse regole, migliori pratiche, protocolli individuati dall'Agenzia cyber francese nella sua veste di supervisore e regolatore.

La soluzione è del resto ragionevole perché codifica sostanzialmente un controllo pubblicistico.

Poiché tornerà utile nei successivi paragrafi, bisogna qui osservare come la tutela dell'anonimato è sì affidata all'ANSSI ma essenzialmente dipende dalla scelta di non avviare un procedimento penale a carico del tester.

Anonimato, responsabilità e azione penale sono infatti un trionomio interdependente: infatti, non v'è vero anonimato se c'è un processo penale da celebrare, e c'è un processo penale solo in presenza di una notizia di reato effettivamente da perseguire.

7. Una scriminante procedurale come possibile porto sicuro per i *penetration tester*?

La soluzione francese è interessante ma così com'è inapplicabile nel nostro ordinamento, non foss'altro perché nella Repubblica Francese l'azione penale è pur sempre discrezionale ed è per questo che lì la condotta del tester può essere valutata secondo un criterio tanto elastico come quello della buona fede (seppur integrata nella sua tipicità dalle disposizioni dell'ANSSI), che invece sarebbe incompatibile con la struttura delle nostrane esimenti penali.

Immaginare nel nostro ordinamento un'area di esenzione della responsabilità richiede anzitutto una impalcatura coerente con il principio di legalità, fondata quindi sulla tipicità delle condotte rilevanti e delle condizioni esimenti sulla scorta delle quali valutare la meritevolezza dell'attività del tester: devono sussistere elementi oggettivi e predeterminati che stabiliscano se e soprattutto in quale proporzione l'offesa arrecata dal test può dirsi giustificata per ragioni di sicurezza cibernetica.

Bisogna anche considerare il ruolo dei soggetti che svolgono i test e la salvaguardia delle ulteriori manifestazioni degli interessi ordinamentali alla sicurezza e all'ordine pubblico.

Per esempio, è più agile immaginare una esimente per chi svolge istituzionalmente attività di sicurezza, quali il personale in ruolo all'Agenzia per la cybersicurezza nazionale o delle forze di polizia data la rilevanza pubblicistica delle relative funzioni e l'esistenza di una disciplina omologa (si pensi, i.e., alla disciplina dell'agente sotto copertura o quella delle cd. garanzie funzionali).

Più complesso risulta invece disciplinare l'attività dei privati, siano essi persone fisiche o giuridiche: per quest'ultimi, si deve contemperare l'esigenza di promuovere l'indipendenza della ricerca e l'anonimato della segnalazione (art. 82 NIS) senza tuttavia giungere ad una liberalizzazione incontrollata di condotte, pur sempre potenzialmente offensive, che potrebbero prestarsi ad usi strumentali.

Emerge, quindi, la necessità di approntare specifici controlli pubblicistici: in questo caso, analogamente all'ANSSI, affidare all'autorità di settore, in sinergia con l'Autorità giudiziaria, il compito di garantire un'ordinata e consapevole gestione delle attività di sicurezza cibernetica attraverso l'adozione di best practices da seguire nell'esecuzione dei test, nella verifica dei relativi risultati e delle metodologie adottate attraverso l'introduzione di eventuali obblighi di comunicazione circa le azioni di *penetration testing* intraprese.

Poiché la NIS 2 richiede un'esenzione che copra le responsabilità penali e civili, la soluzione maggiormente soddisfacente in punto di tutela potrebbe essere quella di introdurre una causa di giustificazione che elimini in radice l'antigiuridicità del fatto commesso, nelle forme della cd. scriminante procedurale, vale a dire quella scriminante che esclude l'antigiuridicità all'esito di una procedura di autorizzazione che si completa prima che il fatto di rilevanza penale venga commesso¹².

In termini generali, rispetto i.e. alle clausole di esclusione della punibilità, la scriminante è oggettiva e agisce sull'antigiuridicità del fatto e, come tale, apporta tutta una serie di benefici in termini di effettività della tutela del *penetration testing*: si estende a tutti i correi eventuali (i.e. all'intero team di hacking); eliminando l'antigiuridicità si escluderebbero anche le conseguenze extra penali

12. V. CONSULICH 2018, p. 38 ss. che in particolare osserva come il modello della scriminante procedurale possa estendersi anche oltre l'ambito delle questioni "eticamente sensibili" nelle quali la categoria si è principalmente sviluppata e SESSA 2023.

della condotta in punto di responsabilità civile e disciplinare¹³.

Nello specifico contesto della sicurezza cibernetica, la predilezione per un modello procedurale di scriminante è data dal fatto che essa consente di meglio incorporare i controlli pubblicistici sulle attività e la garanzia di anonimato¹⁴.

La dinamica procedurale è ben spiegata dalla applicazione della scriminante nel delicato settore dell'autodeterminazione terapeutica, il cd. il suicidio medicalmente assistito: qui le condotte legate a queste pratiche perdono rilevanza penale perché vengono compiute in forza, e in conformità, ad una specifica autorizzazione che è l'epilogo di una procedura volta a valutare in concreto la sussistenza dei presupposti.

In sostanza, con le scriminanti procedurali il soggetto agisce nel rispetto di una disciplina che prevede l'esperimento di controlli pubblicistici preventivi alla condotta, sulla base di parametri di liceità tassativamente predeterminate dalla legge.

Così, il meccanismo di controllo pubblicistico ex ante della scriminante procedurale ha il pregio di consentire un ordinato e vigilato svolgimento di pratiche potenzialmente decettive. Come s'è anticipato, proprio per i penetration test svolti da soggetti terzi ed estranei al produttore/sviluppatore o alle istituzioni, le stesse ragioni di ordine e sicurezza pubblica che giustificano il loro svolgimento impongono di evitare una indiscriminata "liberalizzazione" ma anzi di vagliare, e autorizzare, solo le condotte che risultano meritevoli di non subire conseguenze legali.

Sicché, si potrebbe dunque ipotizzare l'adozione di un decalogo delle pratiche di penetration testing ammissibili e una procedura di autorizzazione preliminare, o meccanismi di notifica e controllo concomitante, affidate all'organo pubblico affinché chi svolge attività di test di sicurezza cibernetica agisca all'interno di un perimetro regolato e tutelato dalla stessa Autorità di settore che, nel sistema italiano, è senz'altro l'Agenzia per la cybersicurezza nazionale.

Infine, come si vedrà nel paragrafo che segue, l'adozione di una scriminante procedurale ha risvolti diretti anche in relazione alla tutela dell'anonimato

del segnalante, l'ultimo pilastro delle politiche di divulgazione coordinata delle vulnerabilità.

8. Anonimato delle segnalazioni e comunicazione della notizia di reato e controllo giudiziario sulle condotte autorizzate

Il terzo pilastro delle politiche di CVD è l'anonimato della segnalazione. Esso è espressamente previsto dalla NIS 2 e ribadito dal già menzionato all'art. 16 del Decreto Legislativo 4 settembre 2024 n.138, a mente del quale il CSIRT Italia ha il compito di assicurare (a richiesta dallo stesso segnalante) l'anonimato delle persone fisiche e giuridiche al momento della segnalazione e nel corso delle azioni successivamente intraprese a seguito della notifica di vulnerabilità.

L'anonimato è parte integrante del generale schema di tutela del tester segnalatore, perché lo mette al riparo dalle possibili conseguenze professionali o legali e quindi lo invoglia a fare test e a condividere nel modo più completo possibile le vulnerabilità identificate, promuovendo la collaborazione e nel complesso contribuendo ad una maggiore sicurezza dei sistemi.

Tuttavia, così congegnato, quest'anonimato risponde solo parzialmente al problema. L'anonimato deve essere infatti letto unitamente ai profili di responsabilità penale e del relativo controllo giudiziario: un segnalatore anonimo ma non scriminato, ad esempio perché non legalmente autorizzato, resta tale fino a quando non viene avviato un procedimento penale volto a verificare la legittimità della sua condotta.

S'è detto¹⁵, infatti, che l'anonimato risulta irrimediabilmente legato alla responsabilità e al promovimento dell'azione penale: se c'è un processo penale da celebrare non c'è anonimato, e se c'è un processo penale significa che si è in presenza di una notizia di reato che è stata comunicata e che incardina il dovere della Procura di procedere conformemente.

La questione è complessa e si apprezza su almeno due livelli: il primo flusso informativo rilevante si attesta nel dovere di comunicare tutte le

13. Sul tema v. FIORINELLI-ZUCCA 2024, p. 9 ss.

14. Anche se bisogna osservare come il modello teorico della scriminante procedurale non sia ancora unanimemente accettato in dottrina v. *supra* CONSULICH 2018.

15. V. *supra* § 6.

informazioni relative ad una potenziale condotta di reato da parte del personale dell'Agenzia cyber alla Procura della Repubblica, secondo il dovere generale stabilito dall'art. 331 c.p.p. c.p.p. a carico dei Pubblici Ufficiali e rafforzato dai doveri di comunicazione introdotti nei decreti cybersicurezza adottati di recente¹⁶; in secondo luogo, vi sono i doveri di ostensione informativa che gravano sulla stessa Procura della Repubblica in sede di iscrizione della notizia di reato e successivo svolgimento delle indagini¹⁷.

Anzitutto, l'ACN, se nel corso delle proprie funzioni ravvisa gli estremi di una condotta di reato, circostanza che in assenza di una specifica disciplina ad hoc per i penetration testing può virtualmente accadere sempre, non può non comunicare alla Procura della Repubblica anche il nome del soggetto segnalatore: il quantum comunicativo è quello della denuncia, la quale contiene, ai sensi dell'art. 332 c.p.p.¹⁸, l'esposizione degli elementi essenziali del fatto e, quando possibile, il domicilio e quanto altro valga alla identificazione della persona alla quale il fatto è attribuito, della persona offesa e di coloro che siano in grado di riferire su circostanze rilevanti per la ricostruzione dei fatti.

A sua volta, la Procura ha il dovere dell'iscrizione nominativa della notizia di reato, atto che è il prodromo necessario all'avvio delle indagini preliminari e infine alla disclosure delle identità del segnalante-autore del test di sicurezza attraverso l'ostensione degli atti di indagine.

Quindi, la notizia di reato espone il segnalatore non solo all'azione investigativa ma soprattutto alla conoscenza della sua identità da parte del produttore/sviluppatore testato che, nella situazione appena descritta, assume senz'altro la posizione di potenziale persona offesa, con conseguente sterilizzazione della funzione di tutela stessa che l'anonimato dovrebbe invece approntare.

Quindi, l'identità del segnalante, prima o poi, è destinata ad emergere. Così accade anche nel

whistleblowing¹⁹, la cui dinamica è prossima a quella ora in commento: l'identità del segnalante è coperta dall'anonimato in relazione e nei limiti del segreto istruttorio dell'art. 329 c.p.p., istituto che è funzionale alla tutela delle indagini e non dei soggetti coinvolti. Per questo, l'anonimato del segnalante è destinato a perdersi senz'altro nel momento in cui le indagini preliminari terminano e, indipendentemente dalla scelta del pubblico ministero sull'esercizio della azione penale, gli atti di indagine vengono messi a disposizione delle parti.

Tuttavia, la situazione si prospetta qui diversa rispetto al whistleblowing: il whistleblower è tendenzialmente il soggetto che ha notizia di una condotta illecita commessa nella struttura dove opera, della quale ha avuto conoscenza in ragione del proprio rapporto di lavoro e che decide di comunicare ai responsabili deputati a ricevere tali segnalazioni che ne assicurano l'anonimato.

Il penetration tester segnalatore, invece, è solitamente colui il quale ha anche commesso le operazioni di test e, quindi, il potenziale fatto stesso di reato, e questo pone il suo anonimato in una posizione decisamente meno resistente di quella del segnalatore testimone.

Per risolvere i segnalati inconvenienti è possibile ipotizzare almeno due soluzioni. La prima si basa sulle ricadute processuali della scriminante procedurale considerata unitamente alle sue ricadute processuali: considerando tale scriminante, il segnalante riceverebbe una tutela decisamente più forte perché, in radice, non ci sarebbe una notizia di reato da comunicare. La seconda, invece, si trae dall'istituto delle garanzie funzionali.

9. L'anonimato attraverso l'assenza di comunicazione della notizia di reato

La prima soluzione è quella legata alle ricadute processuali della causa di giustificazione procedurale: poiché con la scriminante in discorso il fatto

16. In particolare, gli obblighi di trasmettere informazioni rilevanti al Procuratore nazionale antimafia e antiterrorismo relative ai gravi reati informatici inseriti dal comma 1 dell'art. 2-bis del d.l. n. 123/2023 che introduce il nuovo comma 4 dell'art. 17 d.l. n. 82/2021 «Fermo restando quanto previsto dal comma 4, l'Agenzia trasmette al procuratore nazionale antimafia e antiterrorismo i dati, le notizie e le informazioni rilevanti per l'esercizio delle funzioni di cui all'articolo 371-bis del codice di procedura penale». V. NOCERINO 2023.

17. V. APRATI 2010. Per le novità apportate dalla riforma Cartabia v. SCARPINO 2023 e CURTOTTI 2022.

18. V. PAULESU 2023, p. 1524 ss.

19. Secondo le disposizioni della l. 30 novembre 2017, n. 179 e normativa collegata. V. EVARISTI 2021.

è sì tipico ma non antigiuridico già al momento in cui è commesso, in linea di principio non risulta notizia di reato alcuna da comunicare all'ufficio del pubblico ministero, e tanto basta a garantire l'anonimato del *tester*, che evidentemente ha superato positivamente lo scrutinio pubblicistico legato alla scriminante.

In altra prospettiva, questa soluzione lascia comunque spazi di tutela per la persona offesa, verosimilmente il soggetto il cui sistema è stato violato per ragioni di test, che dal canto suo potrebbe nutrire comunque l'interesse all'esercizio dell'azione penale.

Si tratterebbe quindi di prediligere una soluzione di cd. *prosecution by complaint*²⁰ incentrata sull'iniziativa del soggetto target delle operazioni di *penetration testing*: a fronte di una scriminante, è il testato che con la propria denuncia solleciterebbe un sostanziale riesame di quanto compiuto dal tester e, in particolare, del fatto che quest'ultimo abbia agito al di fuori dei limiti di legge.

Il modello di *prosecution by complaint* è di agevole applicazione perché può contare su quanto già disciplinato dal codice di procedura penale: anche a fronte di una condotta scriminata proceduralmente, la persona offesa può comunque trasmettere alla Procura la denuncia di aver subito un'attività di testing illegittima ivi allegando, in modo puntuale, tutti gli elementi utili a rappresentare una notizia di reato quale fatto determinato e non inverosimile riconducibile ad una fattispecie incriminatrice secondo la definizione data dall'art. 335 c.p.p.²¹.

A sua volta il pubblico ministero, ricevuta la denuncia del privato e acquisita la documentazione dell'autorità incaricata dell'autorizzazione, può verificare l'attività di *penetration testing* senza sacrificare l'anonimato del tester, valutando prima

facie se si trova dinanzi ad una notizia di reato o meno.

Se la risposta è negativa, perché non risultano oltrepassati i limiti legali, allora il pubblico ministero può infine iscrivere il fatto non nel registro delle notizie di reato ma in quella dei fatti non costituenti reato (il cd. modello 45 delle pseudo-notizie²²). Per le pseudo-notizie non vigono meccanismi di comunicazione a soggetti diversi dalla Procura che procede all'annotazione, circostanza quest'ultima che ben tutelerebbe gli scopi a cui la ratio dell'anonimato è preordinata: poiché la pseudo notizia riguarda fatti che non hanno rilevanza penale, non ci sono indagini da avviare e, quindi, identità da divulgare alle parti interessate.

Diversamente, se la risposta è positiva, e quindi risulta un'attività di test che eccede o viola le condizioni scriminanti, allora il pubblico ministero procederebbe iscrivendo la notizia di reato e dando avvio alle indagini nelle forme ordinarie.

Del resto, in quest'ultima situazione ci si troverebbe di fronte di un'attività di rilevanza penale da perseguire che, in quanto tale, farebbe venir meno la necessità di tutelare l'anonimato del soggetto che ha agito al di fuori dei limiti legali.

10. L'anonimato e le garanzie funzionali

La seconda possibile soluzione potrebbe essere tratta dalla disciplina delle cd. garanzie funzionali, il nomen con il quale è conosciuta la scriminante speciale disciplinata dagli artt. 17-19 della l. n. 124/2007 che serve ad abilitare gli operatori dei servizi di informazione e sicurezza al compimento di atti costituenti reato laddove quest'ultimi siano necessari per le attività di sicurezza nazionale²³.

Tralasciando i presupposti e le dinamiche applicative, qui rileva in particolare lo speciale regime

20. V. FIORINELLI-ZUCCA 2024, p. 9.

21. Così come recentemente puntualizzata dalla riforma Cartabia al codice di procedura penale. V. CURTOTTI 2022, p. 198 ss.

22. La disciplina delle pseudo notizie si ricava da quella dell'art. 335 c.p.p. per le notizie che costituiscono reato e dall'art. 109 disp. att. c.p.p., il cui combinato disposto abilita le Procure a tenere un registro dove vengono annotati atti e comunicazioni di fatti che non hanno rilevanza penale. La dinamica processuale attesta come nel registro delle pseudo-notizie vengano annotati fatti che, giunti alla procura come notizie solo nominalmente di reato, vengono successivamente accertati come privi di rilevanza penale V. DI BITONTO 2006, p. 113 ss. V. anche SOTTANI 2021; VALENTINI 2020.

23. V. AMATO 2024; RICOTTA 2024, p. 65 ss.; MONTAGNESE-NERI 2016; MOSCA 2008, p. 235 ss. e MARZADURI 2007, p. 735 ss.

di segretezza stabilito per le indagini penali eventualmente avviate su fatti commessi sotto lo scudo delle garanzie: l'art. 19 l. n. 124/2007 prescrive al pubblico ministero di iscrivere la notizia e conservare gli atti di indagine in un separato registro "segreto" allo scopo di preservare l'anonimato degli operatori dei servizi e la riservatezza delle relative attività fintanto che viene verificata la legittimità delle autorizzazioni a commettere reato.

La dinamica processuale dell'istituto è incentrata sulla risoluzione di un conflitto tra poteri che si consuma quando le attività dei servizi sono incise da quelle della magistratura: quando il pubblico ministero si imbatte in un reato commesso dai servizi, avvia una procedura di interpello con il DIS e con il Presidente del consiglio teso a verificare se l'autorizzazione è stata effettivamente rilasciata e il fatto sia stato compiuto entro i limiti di legge. In questo contesto, il segreto serve a tutelare l'integrità delle ragioni di sicurezza nazionale per tutto il corso dell'interpello tra potere esecutivo e giudiziario.

Se la risposta è affermativa, e quindi sussistono i presupposti delle garanzie, il procedimento penale si arresta e quanto documentato nel registro separato ex art. 19 l. n. 124/2007 viene mantenuto segreto ben oltre il corso del procedimento.

Diversamente, se l'autorizzazione manca o eccede i limiti di legge, il procedimento penale, e con esso il regime divulgazione degli atti di indagine, prosegue seguendo il corso ordinario.

Si tratterebbe quindi di mutuare un regime di segretezza ad hoc degli atti di indagine per tutelare l'anonimato dei penetration tester da quello disciplinato dalle garanzie funzionali, ma siffatta soluzione deve essere menzionata per essere esclusa: l'istituto in discorso, e con esso il particolare regime di segretezza del fascicolo preliminare che è parte integrante del complessivo equilibrio normativo, è assolutamente speciale perché giustificato da quelle supreme ragioni di sicurezza nazionale nelle quali si radicano le attività dei Servizi di informazione che le garanzie funzionali sono chiamati a proteggere.

Pertanto, l'istituto, confinato com'è in quello specifico ambito, non può essere spaccettato e fatto oggetto di applicazione estensiva.

11. Conclusioni

Si è ampiamente illustrato come l'assenza di una chiara esenzione legale espone i penetration tester a potenziali responsabilità penali e civili, creando un clima di incertezza che può disincentivare la collaborazione essenziale tra attori pubblici e privati nel campo della cybersicurezza.

La designazione del CSIRT Italia quale organo competente rappresenta un passo importante, ma restano aperte questioni fondamentali che riguardano proprio l'esenzione da responsabilità per i tester di sicurezza e la tutela dell'anonimato dei segnalanti quali pilastri delle politiche di vulnerability disclosure indicati dalla NIS 2.

In questo contesto, l'adozione di una scriminante procedurale emerge come la soluzione più efficace, capace di eliminare l'antigiuridicità delle condotte dei tester quando queste sono svolte in conformità a procedure autorizzate e sotto il controllo dell'autorità competente, in questo caso l'Agenzia per la Cybersicurezza Nazionale, e al tempo stesso tutelare l'anonimato del segnalante sulla scorta delle conseguenze che si verificherebbero nella dinamica processuale.

La tutela dell'anonimato è infatti una garanzia strutturale per la protezione dei tester da possibili ripercussioni legali o professionali e per incentivare la segnalazione tempestiva delle vulnerabilità e, come si è visto, è legato a doppio filo con la dinamica del processo penale che, a sua volta, si impernia sulla rilevanza penale delle condotte di testing.

In definitiva, il pilastro per una politica nazionale di vulnerability disclosure non può che essere un quadro normativo che elimini, o quantomeno minimizzi la rilevanza penale delle attività di testing condotte per finalità legittime, così da rimuovere a cascata gli ostacoli alla tutela della riservatezza da assicurare ai segnalanti, incentivando la cooperazione necessaria per affrontare efficacemente le minacce alla sicurezza cibernetica.

Riferimenti bibliografici

G. AMATO (2024), *Le garanzie funzionali dell'operatore dei servizi di informazione*, in "Sistema penale", 7 novembre 2024

- R. APRATI (2010), *La notizia di reato nella dinamica del procedimento penale*, Jovene, 2010
- A. CADOPPI, S. CANESTRATI, A. MANNA, M. PAPA (a cura di) (2023), *Cybercrime*, Utet, 2023
- F. CONSULICH (2018), *Lo statuto penale delle scriminanti. Principio di legalità e cause di giustificazione: necessità e limiti*, Giappichelli, 2018
- D. CURTOTTI (2022), *L'iscrizione della notizia di reato e il controllo del giudice*, in G. Spangher (a cura di), "La riforma Cartabia", Pacini giuridica, 2022
- M.L. DI BITONTO (2006), *L'avocazione facoltativa*, Giappichelli, 2006
- ENISA (2016), *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*, 2016
- G.M. EVARISTI (2021), *Whistleblowing, tutela dell'anonimato e processo penale: tra limiti costituzionali e orizzonti convenzionali*, in "Diritto Penale e Processo", 2021, n. 7
- G. FIORINELLI, M.V. ZUCCA (2024), *Is the Road to Hell Paved with Good Intentions? A Criminological and Criminal Law Analysis of Prospective Regulation for Ethical Hacking in Italy and the EU*, in G. D'Angelo, F. Luccio, F. Palmieri (a cura di), "Proceedings of the 8th Italian Conference on Cyber Security (ITA-SEC 2024)", paper 45, vol. 3731, CEUR, 2024
- R. FLOR (2020), *Ethical hacker, assolti ma non troppo: le "zone grigie" del diritto penale*, in "Agenda Digitale", 1 ottobre 2020
- R. FLOR (2020-A), *Il diritto penale alla prova dell'hands-on dell'ethical hacking*, in "Diritto di Internet", 2020, n. 1
- A.D. HOUSEHOLDER, G. WASSERMANN, A. MANION, C. KING (2017), *The CERT Guide to Coordinated Vulnerability Disclosure*, Software Engineering Institute, Carnegie Mellon University, 2017
- E. MARZADURI (2007), *Art. 19 - Opposizione della speciale causa di giustificazione all'autorità giudiziaria (commento alla l. n. 3.8.2007 n. 124 - Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto di Stato)*, in "Legislazione penale", 2007, n. 3
- A. MONTAGNESE, C. NERI (2016), *L'evoluzione della sicurezza nazionale in Italia*, in "Sistema di informazione per la sicurezza della Repubblica", 2016
- C. MOSCA (2008), *Le garanzie funzionali*, in C. Mosca, S. Gambacurta, G. Scandone, M. Valentini (a cura di), "I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)", Giuffrè, 2008
- NIS COOPERATION GROUP (2023), *Guidelines on Implementing National Coordinate Vulnerability Disclosure Policies*, 2023
- W. NOCERINO (2023), *Le nuove norme di prevenzione e contrasto alla criminalità informatica*, in "Penale Diritto e Procedura", 9 novembre 2023
- P.P. PAULESU (2023), *Sub Art. 332*, in A. Giarda, G. Spangher (a cura di), "Codice di procedura penale commentato", Wolters Kluwer, 2023
- L. PUPILLO, A. FERREIRA, G. VARISCO (2018), *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges*, CEPS Task Force Reports, 2018
- F.N. RICOTTA (2024), *Arresto e garanzie funzionali nella legge n. 124 del 2007*, in "Rivista giuridica delle forze armate e di polizia", 2024, n. 1
- S. ROSSA (2023), *Cybersicurezza e pubblica amministrazione*, Edizioni Scientifiche Italiane, 2023
- I. SALVADORI (2017), *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "dual-use software"*, in "Rivista italiana di diritto e procedura penale", 2017, n. 2

- D. SCARPINO (2023), *Le innovazioni apportate dalla Riforma Cartabia in tema di iscrizione della notitia criminis*, in “Penale Diritto e Procedura”, 26 luglio 2023
- A. SESSA (2023), *Le giustificazioni procedurali nella teoria del reato*, Edizioni Scientifiche Italiane, 2023
- S. SOTTANI (2021), *Il controllo giudiziale sulle pseudo notizie di reato*, in “Archivio Penale”, 2021, n. 3
- R. URSI (2023), *La sicurezza cibernetica come funzione pubblica*, in R. Ursi (a cura di), “La sicurezza nel cyberspazio”, Franco Angeli, 2023
- C. VALENTINI (2020), *Obbligatorietà dell'azione penale, patologie della prassi e mancanza di controlli*, in “Rivista di diritto processuale”, 2020, n. 3



RIVISTA ITALIANA DI
INFORMATICA E DIRITTO

PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0164 • articolo sottoposto a peer review • pubblicato in anteprima il 6 ago. 2024
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale 

INDRA MACRÌ

Strategie e modelli operativi per la sicurezza delle pubbliche amministrazioni al tempo del PNRR

Il contributo descrive le più recenti indicazioni fornite alle pubbliche amministrazioni a garanzia delle cybersicurezza. L'analisi confronta le differenti disposizioni dirette alle PA in materia di cybersicurezza e ne approfondisce l'ambito di applicazione.

Pubblica amministrazione – Sicurezza cibernetica – Cloud

Strategies and operational models for Public Administrations security at the time of National Recovery and Resilience Plan (RRP)

The paper describes the most recent indications provided to public administrations to guarantee cybersecurity. The analysis compares different provisions for PAs regarding cybersecurity and delves into their scope of application.

Public Administration – Cybersecurity – Cloud

L'Autrice è consigliere dell'area informatica, Servizio studi della Corte costituzionale. Le opinioni espresse nel presente contributo sono riconducibili all'Autrice e non impegnano in alcun modo l'Istituzione di appartenenza

Questo contributo fa parte della sezione monografica *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà*, a cura di Marina Pietrangelo

SOMMARIO: 1. Introduzione. – 2. Le recenti direttive del Presidente del Consiglio dei ministri in materia di cybersicurezza per le PA. – 3. Le precedenti indicazioni alle PA in materia di sicurezza informatica. – 4. I nuovi obblighi di segnalazione e notifica e le PA coinvolte. – 5. Le segnalazioni dell'Agenzia per la cybersicurezza nazionale e i soggetti pubblici e privati coinvolti. – 6. La struttura e il referente per la cybersicurezza. – 7. L'approvvigionamento di beni e servizi ICT in sicurezza. – 8. Il cloud delle pubbliche amministrazioni. – 8.1. *La normativa e la strategia sul cloud delle PA.* – 8.2. *La classificazione dei dati e dei servizi pubblici.* – 8.3. *I livelli minimi delle infrastrutture e dei servizi cloud.* – 8.4. *La migrazione delle PA al cloud.* – 8.5. *L'adeguamento delle infrastrutture e dei servizi, la qualificazione dei servizi cloud.* – 9. Conclusioni.

1. Introduzione

Quando fra il 2020 e il 2021 il nostro Paese ha definito le scelte strategiche da attuare nel Piano nazionale di ripresa e resilienza (PNRR), è partito dalla digitalizzazione, innovazione e messa in sicurezza della PA.

È, infatti, interamente dedicata alla digitalizzazione, innovazione e sicurezza nella PA la prima componente della prima missione del PNRR italiano. Per digitalizzare la PA non basta garantire riservatezza, integrità e disponibilità dei servizi e dei dati pubblici, ma occorre innovare i processi che fino a quel momento hanno governato l'agere pubblico. La digitalizzazione di un pre-esistente servizio "analogico", difatti, non necessariamente produce una riduzione dell'onere burocratico, allorquando, piuttosto che innovare, si pretende di riprodurre in digitale le precedenti procedure analogiche, senza analizzare e valorizzare le nuove opportunità che le tecnologie digitali possono offrire sia nella semplificazione verso cittadini e imprese, sia nello snellimento di processi interni.

Lo sviluppo dei servizi digitali pubblici corre necessariamente sui binari tracciati dall'Europa, poiché il PNRR espressamente stabilisce che gli investimenti digitali delle pubbliche amministrazioni devono essere allineati alle indicazioni in materia fornite dalla Commissione¹. Operazione tutt'altro che facile, visto lo "tsunami normativo europeo" nel settore della digitalizzazione e, in particolare, della cybersicurezza, riflesso nella nostra legislazione per lo più attraverso decreti d'urgenza.

Ad esempio, è contenuto in un decreto d'urgenza² l'obbligo dal 28 febbraio 2021 per le pubbliche amministrazioni di utilizzare come sistemi di identificazione in rete dei cittadini e delle imprese per l'accesso ai servizi digitali pubblici esclusivamente SPID e CIE (e in via residuale la CNS) al posto delle credenziali (utenza e password) rilasciate dalle stesse amministrazioni ai loro utenti.

Ed è sempre attraverso un decreto di urgenza³ che nasce nel 2021 l'Agenzia per la cybersicurezza nazionale (ACN) che si occupa della sicurezza nel campo cibernetico sia di operatori pubblici che privati. Benché siano molti gli attori istituzionali

1. *Piano nazionale di ripresa e resilienza*, p. 12.

2. Cfr. art. 24, co. 1, lett. e) ed f), d.l. 16 luglio 2020, n. 76, *Misure urgenti per la semplificazione e l'innovazione digitale*, convertito dalla legge 11 settembre 2020, n. 120, che ha modificato gli artt. 64 e 64-bis del d.lgs. 7 marzo 2005, n. 82/2005 (*Codice dell'amministrazione digitale*).

3. V. d.l. 14 giugno 2021, n. 82, *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*, convertito dalla l. 4 agosto 2021 n. 105.

con competenze in materia cyber, la stessa *Strategia nazionale di cybersicurezza 2022-2026*, presentata da Mario Draghi, Presidente del Consiglio dei ministri dell'epoca, evidenzia la necessità di un approccio “*whole-of-society*”, che coinvolge anche gli operatori privati, il mondo accademico e della ricerca, nonché la società civile nel suo complesso e la stessa cittadinanza⁴. Anche perché la capillarità e la complessità della società digitale, i suoi effetti sulla sicurezza informatica e, allo stesso tempo, la forte interrelazione fra i molteplici attori richiedono uno sforzo corale e l'impegno del mondo pubblico come di quello privato.

A partire dal 2021, le precedenti funzioni svolte dall'AGID (Agenzia per l'Italia digitale) per la sicurezza cibernetica della pubblica amministrazione digitale sono state trasferite progressivamente all'ACN, che oggi si occupa anche dell'attuazione della strategia cloud pensata a protezione dei dati e dei servizi delle pubbliche amministrazioni.

Come emerge dalla relazione annuale dell'Agenzia per la cybersicurezza nazionale nel 2023 sono stati trattati 1.411 eventi *cyber*⁵, per una media di circa 117 al mese, con un picco di 169 a ottobre. Di questi, 303 sono stati classificati come incidenti⁶, per una media di circa 25 al mese⁷. Occorre osservare, peraltro, che la cybersicurezza, ben prima del PNRR, aveva attirato non solo a livello europeo, ma anche internazionale, l'attenzione del decisore politico. Le tensioni geopolitiche degli ultimi anni, però, hanno intensificato gli attacchi informatici verso quei Paesi, come l'Italia, che nell'ambito della comunità internazionale, hanno assunto *posizioni di solidarietà e sostegno degli attori statuali in*

conflitto sia con riguardo alla crisi russo-ucraina, sia con riguardo allo scenario mediorientale. Partendo da questa considerazione, fra il 2023 e il 2024 sono state pubblicate ben due direttive in materia di cybersicurezza rivolte alle pubbliche amministrazioni, che, tuttavia, come meglio chiarito di seguito, erano già tenute ad attuare specifiche misure in materia di sicurezza informatica.

La legge 28 giugno 2024, n. 90 ha, fra l'altro, ulteriormente rafforzato i compiti assegnati alle amministrazioni pubbliche per cooperare alla difesa cibernetica del Paese.

Nel frattempo, tenuto conto del mutato scenario di rischio, l'Agenzia per la cybersicurezza nazionale ha riordinato la disciplina tecnica in materia di cloud rivolta alle pubbliche amministrazioni, con la pubblicazione lo scorso 27 giugno 2024 del relativo Regolamento⁸, adottato con decreto direttoriale n. 21007/24.

2. Le recenti direttive del Presidente del Consiglio dei ministri in materia di cybersicurezza per le PA

Il Presidente del Consiglio dei ministri, al quale sono attribuite in via esclusiva l'alta direzione e la responsabilità generale delle politiche di cybersicurezza⁹, ha formulato specifiche indicazioni per le pubbliche amministrazioni attraverso le direttive del 6 luglio 2023 e del 29 dicembre 2023, rispettivamente pubblicate nella Gazzetta ufficiale dell'8 agosto 2023 e del 16 febbraio 2024.

La prima direttiva del 6 luglio 2023, diretta alle PA del d.lgs. 30 marzo 2001, n. 165¹⁰, individua indirizzi di coordinamento e organizzazione per

4. ACN 2022, p. 8.

5. Evento cyber è un avvenimento «con potenziale impatto su almeno un soggetto nazionale, ulteriormente analizzato e approfondito, per il quale, in base alle circostanze, il CSIRT Italia dirama alert e/o supporto, eventualmente anche in loco, i soggetti colpiti», Cfr. ACN 2023, p. 11.

6. «Incidente è un evento cyber con impatto su confidenzialità, integrità o disponibilità delle informazioni confermato dalla vittima», *ibidem*.

7. *Ivi*, p. 14.

8. Regolamento per le infrastrutture digitali e per i servizi cloud per la pubblica amministrazione, ai sensi dell'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, per brevità di seguito sarà indicato come “Regolamento cloud ACN” o “Regolamento”.

9. V. art. 2, d.l. n. 82/2021.

10. Restano, però, esclusi dall'ambito di applicazione della direttiva, come per buona parte della disciplina in materia di cybersicurezza, quegli organi dello Stato preposti alla prevenzione, accertamento e repressione dei reati,

una adeguata gestione delle minacce informatiche, degli incidenti e delle situazioni di crisi di natura cibernetica. L'altra direttiva, pubblicata a inizio 2024, invece, è più operativa: fornisce ai ministeri le indicazioni pratiche da seguire per assicurare la resilienza cibernetica del Paese attraverso protocolli di intesa con l'ACN irrobustendo la capacità di risposta agli incidenti informatici.

In particolare nella prima direttiva si stabilisce che le PA garantiscono la massima collaborazione con l'ACN e, specificatamente, con gli operatori del CSIRT Italia¹¹, anche qualora, a seguito di un incidente, vi sia un loro diretto intervento presso la PA. In tal caso è richiesta la piena collaborazione non solo delle pubbliche amministrazioni coinvolte, ma anche delle società *in house* o a controllo pubblico che lavorano a supporto dei sistemi informativi della PA. Tali soggetti dovranno consentire l'accesso ai locali e ai sistemi informativi impattati per tutto il periodo necessario allo svolgimento delle operazioni. L'obiettivo è prendere piena contezza della situazione, anche in considerazione della collaborazione richiesta all'ACN a livello dell'Unione europea in materia di cybersicurezza.

L'ACN, infatti, partecipa ai meccanismi europei di gestione delle crisi cibernetiche, assicurando i collegamenti con le organizzazioni internazionali, di cui l'Italia fa parte, necessari per la gestione delle crisi (art. 10, comma 5, lett. e), d.l. n. 82/2021).

La collaborazione istituzionale è così necessaria in ambito cybersicurezza, tanto più che questa non può essere garantita da un solo soggetto: la complessità della materia richiede la sinergia. Cosicché le indicazioni sulla piena collaborazione contenute nella direttiva del luglio 2023 sono state rafforzate dopo poco, introducendo attraverso una specifica norma¹² sanzioni verso determinati soggetti (anche privati) che non forniscono il pieno supporto alle strutture dell'ACN chiamate a intervenire per le operazioni di contenimento e mitigazione delle conseguenze provocate da un incidente informatico, consentendo il ripristino quanto più tempestivo possibile dell'operatività dei sistemi compromessi.

La successiva direttiva di fine 2023, che, come richiamato, ha un ambito di applicazione più limitato, riferendosi ai soli Ministeri e non a tutte le PA individuate dal d.lgs. n. 165/2001, stabilisce

alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, nonché gli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della l. 3 agosto 2007, n. 124.

11. Ai CSIRT (*Computer security incident response team*) sono attribuiti molteplici compiti, definiti nel d.lgs. 18 maggio 2018, n. 65 e nell'art. 4 del decreto del Presidente del Consiglio dei ministri dell'8 agosto 2019. Essi includono: - il monitoraggio degli incidenti a livello nazionale; - l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti; - l'intervento in caso di incidenti; - l'analisi dinamica dei rischi e degli incidenti; - la sensibilizzazione situazionale; - la partecipazione alla rete dei CSIRT. Il CSIRT stabilisce relazioni di cooperazione con il settore privato e, per facilitare la cooperazione, promuove l'adozione e l'uso di prassi comuni o standardizzate nei settori delle procedure di trattamento degli incidenti e dei rischi e sistemi di classificazione degli incidenti, dei rischi e delle informazioni. Il profilo completo dello CSIRT Italia è contenuto nel documento [RFC 2350](#).
12. Art. 2-bis (*Disposizioni urgenti in materia di contrasto della criminalità informatica e di cybersicurezza*) del d.l. 10 agosto 2023, n. 105, convertito dalla legge 9 ottobre 2023, n. 137, che ha introdotto all'art. 7, co. 1, del d.l. n. 82/2021 la lettera n-bis, per stabilire che la mancata collaborazione con l'ACN da parte dei soggetti pubblici o privati che rientrano nel perimetro di sicurezza nazionale cibernetica (definito dall'art. 1, co. 2, lett. a) del d.l. 21 settembre 2019, n. 105, convertito dalla legge 18 novembre 2019, n. 133, c.d. "Decreto perimetro") che hanno subito incidenti di sicurezza informatica o attacchi informatici è valutata ai fini dell'applicazione delle sanzioni previste dallo stesso decreto perimetro (art. 1, co. 10 e 14 del d.l. n. 105/2019). Tali sanzioni variano da quelle amministrative pecuniarie (fino a euro 1.800.000) alla reclusione (fino a tre anni). Alle stesse sanzioni sono sottoposte, inoltre, gli operatori di servizi essenziali indicati nel d.lgs. 18 maggio 2018, n. 65 (decreto di recepimento della direttiva NIS, cfr. nota n. 16) e le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, come individuate dall'art. 40, d.lgs. 1° agosto 2003, n. 259, *Codice delle comunicazioni elettroniche*. Dall'applicazione della disciplina restano esclusi gli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, nonché gli organismi di informazione per la sicurezza.

anzitutto la necessità di definire al più alto livello istituzionale, ossia fra ciascun Ministro e il vertice dell'ACN, degli atti di intesa, dove si precisano le attività che ciascuno, in caso di attacco informatico subito dal Ministero, è tenuto a svolgere per il contenimento e la mitigazione delle conseguenze dell'incidente informatico. La direttiva, al riguardo, fornisce indicazioni tecnico-organizzative, che costituiscono il presupposto dal quale partire per garantire un ripristino quanto più possibile immediato dell'operatività dei sistemi compromessi delle PA interessate.

Tali indicazioni sono state raggruppate in 4 punti essenziali:

- 1) un censimento dei sistemi hardware e software, oltre che dei flussi di dati utilizzati per lo svolgimento delle attività istituzionali;
- 2) un documento con la definizione di ruoli e responsabilità inerenti alla cybersicurezza, sia per il personale interno, che di terze parti che supportano l'amministrazione, con l'individuazione fra il personale della PA di un incaricato per la cybersicurezza, che sia da punto di contatto con l'ACN, oltre che di un referente tecnico per la cybersicurezza (da identificarsi tra il personale responsabile della gestione operativa dei sistemi informatici);
- 3) dei piani per la gestione delle vulnerabilità, dei backup dei dati necessari per l'esercizio delle proprie funzioni essenziali, nonché del ciclo di vita dei sistemi, delle identità e dei relativi permessi;
- 4) un piano di risposta in caso di incidente, che definisca puntualmente le articolazioni interne che – in stretto raccordo con l'incaricato per la cybersicurezza – sono preposte all'attuazione del piano, definendone le competenze decisionali, finanziarie e tecniche, onde adeguatamente fronteggiare un eventuale incidente cibernetico.

La seconda direttiva, quindi, intende porre l'ACN al fianco delle PA centrali, definendo un "modello operativo", attraverso il quale rispondere molto più efficacemente agli incidenti di sicurezza, evitandone la propagazione e, allo stesso tempo, affida all'ACN medesima il compito di monitorarne l'adozione da parte dei Ministeri.

A ben guardare, come approfondito di seguito, buona parte delle indicazioni contenute nella sopra citata direttiva del Presidente del Consiglio dei ministri pubblicata nel 2024 sono state fornite alle pubbliche amministrazioni già da diversi anni. La vera novità di questa direttiva sta nel fatto che, per garantire la cybersicurezza dei dati e dei servizi pubblici, è investito il più alto vertice dell'amministrazione, ossia lo stesso Ministro e non solo la dirigenza tecnica. La cybersicurezza, quindi, dirompe sempre più in una dimensione politica, non potendo essere contenuta esclusivamente in quella tecnico-amministrativa, dove nella maggioranza dei casi era stata relegata.

3. Le precedenti indicazioni alle PA in materia di sicurezza informatica

Le circolari AGID del 2017 nn. 1 e 2 (la seconda è un aggiornamento della prima) introducono le misure minime di sicurezza e si rivolgono, da ultimo, a tutte le pubbliche amministrazioni indicate dall'art. 2, comma 2 del CAD (*Codice dell'amministrazione digitale*, d.lgs. 7 marzo 2005, n. 82), che comprendeva – alla data di emanazione della circolare n. 2 (18 aprile 2017, G.U. 5 maggio 2017, n. 103) – oltre alle PA individuate dal d.lgs. n. 165/2001, anche le società a controllo pubblico non quotate (art. 2, circolare). La circolare AGID n. 2/2017 stabiliva che l'adozione delle misure minime dovesse avvenire entro il 31 dicembre 2017 (art. 5) e che responsabile dell'attuazione fosse direttamente il Responsabile per la transizione digitale (art. 3). Tali circolari nascono dalla direttiva del Presidente del Consiglio dei ministri del 1° agosto 2015, dove si prevedeva, fra l'altro, che tutte le amministrazioni e gli organi chiamati a intervenire in caso di eventi cibernetici dovessero dotarsi, secondo una tempistica definita e comunque nel più breve tempo possibile, di standard minimi di sicurezza per prevenire e mitigare gli effetti di potenziali attacchi informatici. Nel 2015 la stessa direttiva affidava all'Agenzia per l'Italia digitale la messa a disposizione degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia era parte. Già il 26 aprile 2016 l'AGID in attuazione della citata direttiva aveva pubblicato le *Misure minime di sicurezza ICT*¹³ per le pubbliche amministrazioni come

13. ICT sta per *Information and communication technologies*.

parte integrante delle *Linee Guida per la sicurezza ICT delle Pubbliche Amministrazioni*, richiamando, fra i documenti di riferimento, il CIS, *Critical Security Controls for Effective Cyber Defense* - versione 6.0 di ottobre 2015 e il documento dell'Università La Sapienza del 2015 *Italian Cyber Security Report del CIS*. Quest'ultimo documento, che si ispirava al *Cybersecurity Framework* sviluppato dal *National Institute of Standards and Technology* (NIST), nel 2019 è stato rivisto con il supporto del Garante per la protezione dei dati personali. La nuova versione, *Framework Nazionale per la Cybersecurity e la Data Protection*¹⁴ del febbraio 2019 offre a imprese e pubbliche amministrazioni una guida di supporto nell'implementazione della cybersicurezza allo stesso tempo in linea con le indicazioni in materia di sicurezza contenute nel Regolamento sulla privacy del 2018. Benché non risulti sia stato formalmente recepito con uno specifico provvedimento, tale *Framework* costituisce un riferimento della disciplina regolamentare di settore, tant'è che, ad esempio, è espressamente citato dal Regolamento cloud ACN.

Le misure minime di sicurezza di AGID, formalmente adottate prima come linee guida e poi aggiornate e pubblicate in allegato alla citata circolare, hanno costituito già dal 2016 un'importante guida alla quale amministrazioni pubbliche e gestori di pubblici servizi avrebbero dovuto attenersi. Nel 2019 i loro contenuti sono stati per buona parte ripresi dal *Framework Nazionale per la Cybersecurity e la Data Protection* e poi da ultimo ribaditi nella direttiva del Presidente del Consiglio dei ministri di febbraio 2024.

La Tabella 1 mette a confronto le indicazioni sulla cybersicurezza che negli ultimi anni sono state rivolte alle pubbliche amministrazioni.

Sia la recente direttiva del Presidente del Consiglio dei ministri sia i documenti dell'AGID e il successivo *Framework Nazionale per la Cybersecurity e la Data Protection* prendono le mosse da un concetto base della sicurezza: è possibile difendere solo ciò che si conosce. In tutti i provvedimenti sopra richiamati, pertanto, il primo passo richiesto alle amministrazioni pubbliche è il censimento dei loro beni ICT e la predisposizione di un inventario. Applicando la stessa logica per il passaggio al cloud, come meglio rappresentato di seguito, le pubbliche

amministrazioni hanno dovuto effettuare una preventiva analisi dei propri dati e servizi, classificandoli con riguardo al livello di protezione richiesto dalla loro natura, al fine di definire la tipologia a loro più consona.

La direttiva, peraltro, pone in rilievo la definizione di ruoli e responsabilità, fondamentale per l'applicazione di un altro principio cardine della sicurezza, cosiddetto "*least privilege*". Il principio del privilegio minimo stabilisce che un soggetto dovrebbe avere accesso soltanto a specifici dati, applicazioni o risorse strettamente necessari per il completamento di una determinata attività della quale il soggetto è responsabile. La sua applicazione richiede, quindi, la predisposizione di una mappa aggiornata dove si evidenziano i soggetti, interni ed esterni all'Amministrazione, con i rispettivi ruoli e responsabilità in funzione dei quali è richiesta l'interazione con determinati sistemi hardware e software dell'Amministrazione stessa.

Allineandosi alla normativa tecnica di settore del NIST alla quale si ispirano, tutti i documenti italiani in materia di cybersicurezza messi a confronto presentano l'indicazione per le PA della predisposizione del piano di gestione delle vulnerabilità e del piano di risposta in caso di incidente. L'obiettivo dei piani è quello di avere un'indicazione puntuale e scritta delle azioni da svolgere sia per la fase di protezione alle possibili vulnerabilità sia per la fase più delicata di risposta a un incidente di sicurezza già avvenuto.

Un'importante novità della direttiva, rispetto alla precedente circolare AGID e all'impostazione del Framework (che ha comunque una visione di più ampia prospettiva essendo rivolto tanto a organizzazioni private che pubbliche), sta nell'individuazione di figure professionali dedicate alla sicurezza all'interno dei Ministeri. Se nel 2017 si chiedeva allo stesso Responsabile per la transizione digitale (RTD) lo svolgimento dei compiti connessi agli aspetti di sicurezza, con la nuova direttiva i Ministeri sono chiamati ad individuare fra il loro personale (e non fra quello delle società delle quali eventualmente si servano per il funzionamento dei propri sistemi informativi) un "incaricato per la cybersicurezza". Si tratta di una figura nuova richiesta ai Ministeri, che sia da punto di contatto

14. Cfr. CIS-SAPIENZA-CINI CYBERSECURITY NATIONAL LAB 2019.

Direttiva del PCM del 29 dicembre 2023 (G.U. 16 febbraio 2024)	Misure minime di sicurezza, Circolare AGID (G.U. 5 maggio 2017)	Framework Nazionale per la Cybersecurity e la Data Protection
censimento dei sistemi hardware e software, oltre che dei flussi di dati utilizzati per lo svolgimento delle attività istituzionali	inventario delle risorse hardware e software (all. 1 alla circolare, ABSC1 e ABSC2); analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica (all. 1 alla circolare, ABSC13).	inventario di dispositivi e software (Appendice A, ID.AM - 1-5)
definizione di ruoli e responsabilità inerenti alla cybersicurezza, sia per il personale interno, che di terze parti che supportano l'amministrazione, con l'individuazione fra il personale della PA di un incaricato per la cybersicurezza, che sia da punto di contatto con l'ACN, oltre che di un referente tecnico per la cybersicurezza (da identificarsi tra il personale responsabile della gestione operativa dei sistemi IT)	uso appropriato dei privilegi di amministratore: - assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse; - tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona (all. 1 alla circolare ABSC 5)	sono definiti e resi noti ruoli e responsabilità inerenti alla cybersecurity, al trattamento e alla protezione dei dati per tutto il personale e per eventuali terze parti rilevanti (es., fornitori, clienti, partner) (ID.AM - 6-7)
piani per la gestione delle vulnerabilità; backup dei dati necessari per l'esercizio delle proprie funzioni essenziali, nonché del ciclo di vita dei sistemi; identità e relativi permessi	valutazione e correzione continua della vulnerabilità: definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (all. 1 alla circolare, ABSC4); copie di sicurezza (all. 1 alla circolare, ABSC10)	i backup delle informazioni sono eseguiti, amministrati e verificati; viene sviluppato e implementato un piano di gestione delle vulnerabilità; le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza (allegato A, PR.IP-4, PR.IP-12; PR.AC-1)
piano di risposta in caso di incidente, nel quale vengano puntualmente definite le articolazioni interne che – in stretto raccordo con l'incaricato per la cybersicurezza – sono preposte all'attuazione del piano, definendone le competenze decisionali, finanziarie e tecniche, onde adeguatamente fronteggiare un incidente cibernetico.	difese contro i malware: implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate (all. 1 alla circolare ABSC8)	sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro (PR.IP-9)

TAB. 1 — *Confronto fra i provvedimenti in materia di cybersicurezza rivolti alle PA (2016-2024)*

con l'ACN. Tale figura, secondo la direttiva, deve essere affiancata da un referente tecnico per la cybersicurezza, che dovendo essere individuato fra

il personale responsabile della gestione operativa dei sistemi IT, potrà anche essere estraneo all'Amministrazione. Le figure professionali dedicate alla

cybersicurezza che i Ministeri destinatari della direttiva dovranno individuare integrano le funzioni in materia di sicurezza, che la norma da sempre assegna all'Ufficio per la transizione digitale. In particolare il CAD stabilisce che all'Ufficio del Responsabile per la transizione digitale siano affidati i compiti di indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture (art. 17, co. 1, lett. c). Sotto il profilo organizzativo, con riferimento alle figure specializzate in materia di cybersicurezza delle quali le pubbliche amministrazioni devono dotarsi, la direttiva anticipa le indicazioni contenute nella nuova legge varata per il rafforzamento della cybersicurezza nazionale, l. 90/2024, di seguito illustrate.

4. I nuovi obblighi di segnalazione e notifica e le PA coinvolte

Il recente provvedimento legislativo in materia di cybersicurezza in vigore dal 17 luglio 2024 stabilisce che le pubbliche amministrazioni segnalano, secondo modalità predefinite, gli incidenti di sicurezza aventi impatto su reti, sistemi informativi e servizi informatici. Per agevolare la comunicazione con l'ACN, i soggetti che hanno subito un incidente informatico sono tenuti alla segnalazione e notificazione facendo riferimento alla tassonomia descrittiva degli eventi informatici adottata con apposito provvedimento dell'ACN¹⁵ (art. 1, comma 1, l. n. 90/2024). La tassonomia è una sorta di vocabolario degli incidenti di sicurezza più gravi, che richiedono un intervento immediato per il contenimento dei loro effetti. Le amministrazioni malcapitate dovranno collegarsi al sito dell'ACN per effettuare la segnalazione entro 24 ore dall'accaduto, fornendo entro

72 ore – che la norma espressamente fa decorrere dallo stesso momento – informazioni complete in sede di notifica (art. 1, co. 2, l. n. 90/2024). Mentre le PA centrali sono tenute all'attuazione delle disposizioni sopra richiamate dalla loro entrata in vigore, le restanti, invece, avranno più tempo per adeguarsi, poiché la norma prevede per loro l'entrata in vigore dopo centottanta giorni (art. 1, co. 3, l. n. 90/2024). Qualora l'evento non rientri nella tassonomia sopra richiamata, le PA coinvolte possono comunque procedere alla segnalazione, secondo la disciplina della notifica volontaria, introdotta con il decreto di recepimento della direttiva NIS¹⁶ (art. 1, co. 4, l. n. 90/2024).

L'attenzione del legislatore sulle attività di notifica è forte, anche in considerazione dell'intensificarsi della minaccia cyber, al punto tale che sono previste visite ispettive – da disciplinarsi con un successivo provvedimento dell'ACN – e, nei casi di reiterata inosservanza, sanzioni pecuniarie fino a 125.000 euro a carico delle amministrazioni inadempienti rispetto all'obbligo di notifica, oltre alla responsabilità disciplinare e amministrativo-contabile non limitata ai soli dirigenti, ma anche ai funzionari responsabili (art. 1, co. 5 e 6, l. n. 90/2024).

La legge n. 90/2024 si rivolge a una pluralità di amministrazioni:

- pubbliche amministrazioni centrali individuate dall'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196;
- regioni, province autonome di Trento e di Bolzano, città metropolitane, comuni con popolazione superiore a 100.000 abitanti e, comunque, comuni capoluoghi di regione;
- società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane;

15. Determina 3 gennaio 2023, contenente la *Tassonomia degli incidenti che debbono essere oggetto di notifica*. L'allegato associa un codice identificativo a ciascuna tipologia di incidente (es. con il codice "ICP-C-1" è indicato l'incidente così descritto in tassonomia: «Il soggetto ha evidenza dell'effettivo accesso non autorizzato all'interno della rete attraverso vettori di infezione, lo sfruttamento di vulnerabilità di risorse esposte pubblicamente o qualsiasi altra tecnica nota»).

16. La direttiva cosiddetta NIS (direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione) è stata recepita in Italia con il d.lgs. 65/2018, che all'art. 18 stabilisce, fra l'altro, che il CSIRT Italia tratti le notifiche volontarie con priorità inferiore rispetto a quelle obbligatorie e soltanto qualora tale trattamento non costituisca un onere sproporzionato o eccessivo. Il soggetto notificante, a sua volta, non è sottoposto a nessuno degli obblighi a cui non sarebbe stato sottoposto se non avesse effettuato tale notifica.

- aziende sanitarie locali;
- società in house delle sopra richiamate amministrazioni che forniscono servizi informatici, servizi di trasporto ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, o di gestione dei rifiuti (art. 1, co. 1, l. n. 90/2024).

Lo stesso articolo individua, altresì, i soggetti che non sono tenuti all'attuazione del medesimo articolo 1 (art. 1, co. 7, l. n. 90/2024)¹⁷.

La richiamata disposizione individua in questo modo un ambito di applicazione per alcuni versi nuovo e, comunque, non direttamente sovrapponibile con quello cui si riferiscono le principali norme nel settore della digitalizzazione della pubblica amministrazione.

La legge n. 90/2024, in particolare, per le PA centrali si riferisce alla legge in materia di contabilità e finanza pubblica, l. n. 196/2009 che, a sua volta, rimanda alla lista S.13. La lista S.13 – largamente utilizzata nell'ambito della contabilità e finanza pubblica – per quanto attiene alla disciplina di

digitalizzazione delle PA, invece, viene utilizzata per la prima volta nel 2020 con riferimento all'obbligo delle PA alla migrazione al cloud¹⁸. Definita annualmente dall'ISTAT e pubblicata in Gazzetta ufficiale per la sua importante valenza economico finanziaria – in quanto costituisce il riferimento per l'elaborazione dei conti economici nazionali e del conto economico consolidato delle amministrazioni pubbliche, che sono alla base del calcolo degli indicatori trasmessi dall'Istat alla Commissione europea, in applicazione del Protocollo sulla procedura per i deficit eccessivi annesso al Trattato di Maastricht – la lista S.13 risulta composta da tre sotto settori:

- “Amministrazioni centrali”;
- “Amministrazioni locali”;
- “Enti nazionali di previdenza e assistenza”¹⁹.

Nel definire il perimetro di applicazione, la legge n. 90/2024 cita espressamente le “Amministrazioni centrali” della lista S.13, con ciò escludendo le rimanenti amministrazioni ivi elencate, ossia le “Amministrazioni locali” e gli “Enti nazionali di

17. Sono espressamente escluse dall'applicazione del solo articolo 1 della l. n. 90/2024: - operatori di servizi essenziali, intesi come soggetti pubblici o privati del settore dell'energia elettrica, petrolio, gas; settore del trasporto aereo, ferroviario e marittimo, oltre che stradale (limitatamente alle sole “autorità stradale”, ossia qualsiasi autorità pubblica responsabile della pianificazione, del controllo o della gestione delle strade, come definita dall'articolo 2, punto 12, del regolamento delegato (UE) 2015/962 della Commissione e i gestori di sistemi di trasporto intelligente definiti all'art. 1, co. 1, lett. a), del decreto del Ministro delle infrastrutture e dei trasporti 1 febbraio 2013); settore bancario; settore delle infrastrutture dei mercati finanziari; istituti sanitari compreso ospedali e cliniche; fornitori e distributori di acqua potabile; operatori nel settore delle infrastrutture digitali (essenzialmente gli operatori indispensabili per il funzionamento della rete Internet); fornitori di servizi digitali (art. 3, co. 1, lett. g) ed i) del d.lgs. 18 maggio 2018, n. 65, con il quale è stata recepita la direttiva NIS che sarà abrogata a partire dal 18 ottobre 2024). Per la definizione di “fornitori di servizi digitali” il decreto di recepimento della direttiva NIS non offre una chiara definizione, rinviando a quella di “servizio digitale” contenuta nella direttiva dir. n. 2015/1535 (direttiva del Parlamento europeo e del Consiglio che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione) dove all'art. 1, par. 1, si definisce il servizio digitale come «qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi»; - i soggetti elencati nel perimetro di cybersicurezza nazionale (art. 1, co. 2-bis, del d.l. n. 105/2019). Tale elenco è adottato con un atto amministrativo non soggetto a pubblicazione (ed escluso dal diritto di accesso), fermo restando che a ciascun soggetto è data, separatamente, comunicazione senza ritardo dell'avvenuta iscrizione nell'elenco (art. 1, co. 7, lett. a), l. n. 90/2024). Inoltre sono esclusi dall'attuazione dell'art. 1, co. 1 della l. n. 90/2024 anche gli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato e agli organismi di informazione per la sicurezza (art. 1, co. 7, lett. b), l. n. 90/2024).

18. Art. 33-septies, d.l. n. 179/2012, come modificato dall'art. 35, co. 1, lett. a), d.l. 16 luglio 2020, n. 76, convertito, dalla l. 11 settembre 2020, n. 120.

19. ISTAT 2023.

previdenza e assistenza”, come ad esempio INPS, INAIL, ecc. Con riguardo alle PA centrali, quindi, la legge n. 90/2024 si estenderebbe astrattamente (a meno di esclusioni derivanti dall'appartenenza al perimetro di sicurezza nazionale) anche agli organi costituzionali, che sono, ad esempio, esclusi dall'applicazione del CAD, ma rientrano, viceversa, nell'ambito di applicazione della disciplina in materia di cloud, in quanto appartenenti alla lista S.13 (art. 33-*septies* del d.l. 18 ottobre 2012, n. 179, convertito dalla l. 17 dicembre 2012, n. 221). Per quanto attiene alle pubbliche amministrazioni locali, la legge n. 90/2024 non si applica a tutte quelle elencate nella lista S.13, ma a un loro sottoinsieme: determinati comuni, individuati sulla base della maggiore numerosità della popolazione residente o dell'essere capoluogo di regione, e le aziende sanitarie. L'interpretazione letterale dell'ambito di applicazione così definito dalla legge n. 90/2024, infine, porterebbe ad escludere in ogni caso gli enti previdenziali e assistenziali. Tali enti, infatti, non sono inclusi in nessuna delle fattispecie sopra elencate, essendo classificati dalla lista S.13 come “Enti nazionali di previdenza ed assistenza”, pur rientrando, tuttavia, nell'ambito di applicazione del CAD, in quanto assoggettati al d.lgs. 30 marzo 2001, n. 165²⁰.

Se, dunque, l'ambito di applicazione della legge n. 90/2024 è restrittivo con riguardo alle pubbliche amministrazioni territoriali – in quanto esclude quelle di dimensioni inferiori ai 100.000 abitanti, a meno che non siano capoluoghi di regione

(Ancona, Aosta, Campobasso, Catanzaro, L'Aquila, Potenza) – con riguardo alle pubbliche amministrazioni centrali, invece, copre una superficie differente da quelle indicata dal CAD.

Altra caratteristica dell'ambito di applicazione della legge n. 90/2024 è rappresentata dall'inclusione di un insieme di aziende definite sulla base della tipologia dell'attività economica svolta: sanità, trasporto pubblico, raccolta, smaltimento o trattamento di acque, gestione dei rifiuti. Si tratta di un'impostazione già presente nella direttiva NIS, ma rafforzata nella direttiva cosiddetta NIS 2²¹, in corso di adozione in Italia, che, nell'aggiornare la precedente direttiva NIS, intende, fra l'altro, omogeneizzare fra gli Stati membri l'ambito di applicazione, la cui delimitazione è stata lasciata alla loro discrezione. Una delle principali novità della nuova direttiva NIS sta proprio nell'aver esteso il suo ambito di applicazione prevedendovi, fra l'altro, espressamente le pubbliche amministrazioni²². Ciò anche a dimostrazione di quanto la cybersicurezza sia un tema sempre più centrale nell'attività amministrativa degli Stati membri.

La Tabella 2, prendendo a riferimento le principali norme rivolte alle PA in materia di digitalizzazione e cybersicurezza (CAD, disciplina in materia di cloud e la recente disciplina sulla cybersicurezza) riassume il relativo ambito di applicazione.

Per quanto limitata, l'analisi sull'ambito di applicazione delle discipline in materie di digitalizzazione e sicurezza, sopra brevemente illustrata, mostra da un lato la delicatezza con la

20. Gli atti parlamentari, peraltro, con riferimento all'ambito di applicazione non forniscono ulteriori indicazioni (atti parlamentari Camera dei deputati, AC 1717, presentato il 17 febbraio 2024).

21. [Direttiva \(UE\) 2022/2555](#) del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.

22. La direttiva NIS2 distingue i soggetti che entrano nel novero di applicazione della direttiva NIS2 in essenziali ed importanti, individuando per essi due regimi differenti. Lo sforzo richiesto alle organizzazioni per l'attuazione della disciplina in materia di cybersicurezza, infatti, è considerevole, cosicché sulla base del tipo di servizio erogato e della sua criticità in caso di interruzione, sono definite misure di protezione differenti. La direttiva definisce le PAC soggetti essenziali e le PAL soggetti importanti, salvo che il singolo Stato membro non le definisca essenziali. Ciascuno Stato membro può identificare una pubblica amministrazione regionale come soggetto essenziale quando il Paese ritenga che tale amministrazione rientri in una delle seguenti casistiche: - rappresenta l'unico fornitore di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali; - una perturbazione del servizio fornito da tale amministrazione potrebbe avere un impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica o potrebbe comportare un rischio sistemico significativo, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero; - risulta critica in ragione della sua particolare importanza a livello nazionale o regionale.

		NORME IN MATERIA DI DIGITALIZZAZIONE E CYBERSICUREZZA DELLE PA		
		CAD (d.lgs. n. 82/2005)	art. 33-septies, d.l. n. 179/2012	legge n. 90/2024 (art. 1)
TIPOLOGIA DI PA CUI SI APPLICA LA DISCIPLINA SU DIGITALIZZAZIONE E CYBERSICUREZZA	PAC lista S.13	X (1)	X	X (8)
	PAL lista S.13	X (2)	X	Solo aziende sanitarie locali e comuni al di sopra dei 100.000 abitanti o capoluoghi di regione
	enti nazionali di previdenza e assistenza	X (3)		
	autorità amministrative indipendenti di garanzia, vigilanza e regolazione	X	X (4)	X (10)
	gestori di servizi pubblici	X	X (9)	X (5)
	società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175	X (6)	X (9)	X (7)
(1) purché assoggettati al d.lgs. n. 165/2001 o autorità indipendenti (2) purché assoggettati al d.lgs. n. 165/2001 o autorità di sistema portuale (3) purché assoggettati al d.lgs. n. 165/2001 (4) limitatamente a quelle indicate fra le "Autorità indipendenti" della lista S.13: sono, ad esempio, incluse l'Autorità garante della concorrenza e del mercato, l'Autorità per le garanzie nelle comunicazioni, ma escluse dalla lista S.13 Consob (Commissione nazionale per la società e la borsa, che è l'autorità italiana per la vigilanza dei mercati finanziari) e IVASS (Istituto per la vigilanza sulle assicurazioni, che è un'autorità indipendente) (5) limitatamente ai servizi di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti e di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane, purché non presenti nell'elenco del perimetro di sicurezza nazionale (articolo 1, comma 2-bis, del decreto-legge 21 settembre 2019, n. 105, convertito dalla legge 18 novembre 2019, n. 133) (6) escluso le società quotate (7) limitatamente alle società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane e alle società in house delle amministrazioni oggetto della L. n. 90/2024 che forniscono servizi informatici, servizi di trasporto ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, o di gestione dei rifiuti, purché non presenti nell'elenco del perimetro di sicurezza nazionale (articolo 1, comma 2-bis, del d.l. n. 105/2019) (8) purché non presenti nell'elenco del perimetro di sicurezza nazionale (articolo 1, comma 2-bis, del d.l. n. 105/2019) (9) purché presenti nella lista S.13, sottosettore "Amministrazioni centrali" o "Amministrazioni locali" (10) limitatamente a quelle indicate fra le "Autorità indipendenti" della lista S.13, purché non presenti nell'elenco del perimetro di sicurezza nazionale				

TAB. 2 — *Tipologia di PA cui si applicano le norme in materia di digitalizzazione e cybersicurezza*

quale occorre intervenire laddove nuovi oneri sono posti in capo alle amministrazioni spesso costrette a fronteggiare le nuove disposizioni con personale ridotto, dall'altro la difficoltà

di omogeneizzazione in una materia travolta in questi ultimi anni da una convulsa produzione normativa, che allo stato, non ha ancora trovato l'auspicabile sintesi²³.

23. Cfr. al riguardo anche LONGO 2024 che ha ribadito la necessità di un coordinamento tra le norme attuali e le emanande disposizioni del decreto legislativo di attuazione [NIS2] nella sua Audizione informale per il disegno

5. Le segnalazioni dell'Agenzia per la cybersicurezza nazionale e i soggetti pubblici e privati coinvolti

Oltre alle segnalazioni *ex-post* che le PA devono effettuare all'ACN in caso di incidente, la legge individua anche la possibilità che *ex-ante* sia l'Agenzia per la cybersicurezza nazionale a segnalare specifiche vulnerabilità cui le PA possono essere esposte. In tal caso le PA sono tenute ad adottare sollecitamente tutti gli accorgimenti indicati dalla stessa ACN e comunque entro quindici giorni. Deroghe a tali termini sono consentite solo qualora vi siano « motivate esigenze di natura tecnico-organizzativa » per le quali non sia possibile provvedere o procedere nei termini indicati. Tali motivate esigenze, in ogni caso, la PA deve farsi carico di comunicarle tempestivamente all'ACN, pena l'applicazione di sanzioni (art. 2, l. n. 90/2024).

Le disposizioni sopra richiamate sono valide non solo per tutte le pubbliche amministrazioni centrali della lista S.13, regioni, province autonome di Trento e di Bolzano, città metropolitane, comuni con popolazione superiore a 100.000 abitanti e, comunque, comuni capoluoghi di regione, società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane, aziende sanitarie locali, società in house delle sopra richiamate amministrazioni che forniscono servizi informatici, servizi di trasporto ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, o di gestione dei rifiuti, ma anche per tutti i soggetti, quindi sia pubblici che privati, espressamente esclusi dall'ambito di applicazione dell'articolo 1

della legge n. 90/2024, ossia i soggetti presenti nell'elenco che costituisce il perimetro di cybersicurezza nazionale, gli operatori pubblici o privati di servizi essenziali, quali ad esempio trasporto ed energia (*amplius* nota 17), oltre che le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico (art. 2, co. 1, l. 90/2024).

6. La struttura e il referente per la cybersicurezza

Le PA centrali e locali, oltre che i gestori di pubblici servizi e le in house, definite nell'art. 1 della legge n. 90/2024, senza nuovi oneri individuano una nuova struttura, qualora non già presente, che segua la cybersicurezza (art. 8, l. n. 90/2024²⁴). La norma elenca puntualmente le funzioni, che vanno dallo sviluppo delle politiche e procedure di sicurezza alla predisposizione di un piano per la gestione del rischio informatico, oltre che la definizione in un apposito documento dei ruoli e dell'organizzazione del sistema per la sicurezza delle informazioni della PA. La struttura è anche responsabile per la predisposizione di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione da tenere aggiornato, che tenga anche conto della pianificazione di specifici interventi da realizzare per aumentare la capacità nella gestione dei rischi cibernetici. È assegnato a tale struttura, inoltre, il compito di dare attuazione alle linee guida per la cybersicurezza emanate dall'ACN²⁵, oltre che il monitoraggio e la valutazione continua delle minacce e delle vulnerabilità. Si tratta di adempimenti non nuovi per le amministrazioni, in quanto allineati alle indicazioni del NIST. Presso tale struttura la norma ha stabilito che sia operativo un referente per la cybersicurezza, con specifiche

di legge in materia di « Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici » (AC 1717).

24. L'ambito di applicazione dell'art. 8 della l. n. 90/2024 rinvia a quello dell'art. 1 della stessa legge, a esclusione non di tutte le PA indicate nell'art. 1, co. 7 (cfr. nota 17), ma di un insieme più piccolo. Sono esclusi dall'ambito di applicazione dell'art. 8 della legge n. 90/2024 solo i soggetti inseriti nel perimetro di cybersicurezza nazionale e gli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato e agli organismi di informazione per la sicurezza (art. 8, co. 6, l. n. 90/2024).

25. Come espressamente previsto dall'art. 9 della l. n. 90/2024 dovranno essere attuate le linee guida di ACN in materia di crittografia e conservazione delle password (quest'ultime adottate insieme al Garante per la protezione dei dati personali), verificando che non comportino vulnerabilità note, atte a rendere disponibili e intellegibili a terzi i dati cifrati. Tale disposizione si estende anche ai soggetti inclusi nel perimetro e a quelli indicati nella disciplina di attuazione della NIS.

e comprovate professionalità e competenze in materia, che rappresenta il punto di contatto unico dell'amministrazione con l'ACN (art. 8, commi 1 e 2, l. n. 90/2024). In questo modo la norma delinea la necessità, già percepita da diverse istituzioni non solo private, di individuare la figura, generalmente indicata con l'acronimo di CISO (*Chief information security officer*), che recentemente in Italia si è organizzata in associazione²⁶.

Fermo restando che la struttura descritta e il referente per la cybersicurezza possono coincidere rispettivamente con l'Ufficio per la transizione digitale (UTD) e il suo responsabile (RTD), il legislatore, nella piena consapevolezza della ridotta disponibilità di personale tecnico nella PA, introduce ulteriori opzioni. Anzitutto stabilisce la possibilità di conferire l'incarico di referente per la cybersicurezza a un dipendente di un'altra PA, previo l'autorizzazione di quest'ultima (art. 8, co. 3, l. n. 90/2024) e poi, analogamente alle funzioni di RTD e UTD ne prevede la "forma associata", richiamando espressamente le indicazioni del CAD in materia (art. 8, co. 4, l. n. 90/2024). Quello della "forma associata" è un istituto pensato nel CAD prevalentemente per le PA di dimensioni ridotte, comunque diverse dalle "Amministrazioni dello Stato" che, avendo difficoltà a reperire personale qualificato nei loro ruoli, attraverso un'apposita convenzione definiscono l'UTD e nominano l'RTD insieme, in modo che l'ufficio e il suo responsabile provvedano allo stesso tempo alle esigenze di più amministrazioni. Per supportare le PA nell'attuazione pratica della costituzione dell'UTD e della nomina dell'RTD in forma associata, AGID ha predisposto un apposito *Vademecum* pubblicato lo scorso giugno. Come lascia intendere lo stesso schema di convenzione allegato al *Vademecum* e la formulazione recentemente novellata del comma 1-*septies* dell'art. 17 CAD, per la nomina dell'RTD in forma associata si può ricorrere anche a personale delle società in house. Pertanto è possibile dedurre anche per la nomina del referente della cybersicurezza che le PA possano farlo in forma associata

per il tramite delle loro *in house*²⁷. L'obiettivo complessivo è aumentare la resilienza delle PA, motivo per cui la norma assegna all'ACN anche il potere di definire ulteriori modalità e processi di coordinamento e di collaborazione tra le amministrazioni e i referenti per la cybersicurezza (art. 8, co. 5, l. n. 90/2024). In altri termini è ipotizzabile immaginare che laddove le PA per motivi organizzativi non riescano a definire un loro referente, sia la stessa ACN a dettare le modalità operative alternative per garantire il coordinamento in materia cyber.

7. L'approvvigionamento di beni e servizi ICT in sicurezza

Ulteriori adempimenti delle amministrazioni, infine, riguardano l'approvvigionamento di beni e servizi informatici da impiegarsi per la tutela degli interessi nazionali strategici o per la tutela della sicurezza nazionale. L'art. 14 della l. n. 90/2024 stabilisce che con un decreto del Presidente del Consiglio dei ministri saranno individuate specifiche categorie tecnologiche di beni e servizi informatici per le quali devono essere previsti criteri premianti, laddove le proposte o le offerte relative contemplino l'uso di tecnologie di cybersicurezza italiane o di specifici Paesi (appartenenti all'Unione europea o aderenti all'Alleanza atlantica, ecc.). La disposizione sopra richiamata si rivolge a un altro gruppo di amministrazioni, ed esattamente a quelle che costituiscono l'ambito di applicazione del CAD. In attesa che il decreto attuativo chiarisca le forniture cui si applica la disposizione introdotta dalla legge n. 90/2024, è evidente che la norma sopra richiamata intende non solo proteggere le forniture italiane ed europee, ma soprattutto promuovere tecnologie italiane o di Paesi alleati, che, rispetto a quelle di Paesi terzi, possono offrire maggiori garanzie in caso di problemi di sicurezza.

8. Il cloud delle pubbliche amministrazioni

Quando il cloud si è affacciato sul mercato italiano e AGID ne ha previsto l'adozione per le pubbliche

26. *Associso*.

27. Nel richiamare espressamente anche il comma 1-*sexies* dell'art. 17 CAD, probabilmente il legislatore intende limitare l'applicazione di questa disposizione alle sole PA non statali fra quelle individuate dall'art. 1, co. 1, l. n. 90/2024.

amministrazioni²⁸, come spesso accade per le nuove tecnologie, un certo gruppo di “addetti” l’ha accolto con ostilità. Quasi sistematicamente in riunioni informali, convegni o seminari veniva sollevata la questione della “sicurezza” del cloud. Il dibattito, quando non sfociava in scenari di apocalittica manipolazione, oscillava comunque fra l’inaccettabile incertezza del luogo dove fisicamente il dato (o il servizio) pubblico erano ospitati e la convinta repulsione verso potenze straniere, detentrici delle tecnologie cloud che avrebbero potuto immagazzinare quel dato, facendone automaticamente vacillare la sovranità. Nel frattempo che la diffidenza sulle tecnologie cloud si sviluppava in modalità per certi versi pretestuosamente ottusa, la naturale obsolescenza delle infrastrutture pubbliche e/o gli attacchi di sicurezza colpivano dati e servizi digitali delle pubbliche amministrazioni nella loro riservatezza, integrità o affidabilità.

I dati e i servizi della pubblica amministrazione oggi sono considerati i nuovi beni pubblici da proteggere adeguatamente. Cosicché già nell’edizione 2019-2021 il piano triennale per l’informatica nella PA introduce il principio *cloud first*, invitando le pubbliche amministrazioni a utilizzare prioritariamente soluzioni cloud. Le tecnologie cloud, fino a poco prima catalogate come anello debole della catena di sicurezza digitale della PA, vengono collocate fra le tecnologie obbligatorie, in quanto abilitanti a garantire la riservatezza, ma soprattutto disponibilità e integrità delle informazioni pubbliche. A tal fine il PNRR dedica i primi due

investimenti della prima componente della prima missione al cloud, con uno stanziamento iniziale di circa 2 miliardi di euro²⁹. Dopo poco, con la presentazione a settembre 2021 della strategia del Governo italiano sul cloud della pubblica amministrazione, la visione sulle tecnologie cloud è completamente ribaltata: da elemento di erosione a pilastro imprescindibile per la cybersicurezza delle pubbliche amministrazioni.

8.1. La normativa e la strategia sul cloud delle PA

La norma in materia di cloud è contenuta all’interno dell’art. 33-*septies* del d.l. n. 179/2012, che ha subito fino al 2021 diverse modifiche. L’attuale rubrica dell’articolo 33-*septies* “Consolidamento e razionalizzazione dei siti e delle infrastrutture digitali del Paese”, che corrisponde a quella originariamente attribuita alla disposizione inserita in sede di conversione del d.l. n. 179/2012, conserva al suo interno la finalità originaria per la quale è stato introdotto il cloud nella pubblica amministrazione: condividere le risorse infrastrutturali delle pubbliche amministrazioni per raggiungere risparmi di spesa. Il provvedimento originario, peraltro, era stato inserito all’interno di uno dei decreti d’urgenza del Governo Monti, che intendevano sostenere l’innovazione per la crescita del Paese³⁰. Già nello scorso decennio, infatti, si puntava al digitale, come volano per far ripartire l’economia italiana, duramente provata dalla crisi finanziaria del 2011.

28. Il Piano triennale nel 2017-2019 indicava come «le Infrastrutture fisiche perseguono l’obiettivo di aumentare la sicurezza, ridurre il costo delle infrastrutture tecnologiche e migliorare la qualità dei servizi software della Pubblica amministrazione, attraverso la razionalizzazione dei data center, l’adozione sistematica del paradigma cloud e lo sviluppo della connettività», prevedendo che «la realizzazione del cloud della PA» avrebbe consentito di virtualizzare «il parco macchine di tutte le Pubbliche amministrazioni, con importanti benefici in termini di costi e di gestione della manutenzione». Già nel 2017 con la circolare n. 5/2017 l’AGID introduce il tema del cloud per le pubbliche amministrazioni. L’AGID successivamente avvia il censimento dei data center con il quale si mette a nudo tutta la fragilità delle infrastrutture utilizzate dalle PA. Cosicché con la circolare n. 1 del 14 giugno 2019 viene previsto l’obbligo di “migrare senza indugio al Cloud della PA” per quelle PA, che costituivano la stragrande maggioranza, con data center dalle caratteristiche tecniche inadeguate.

29. In particolare 900 milioni di euro sono stati dedicati alla realizzazione del Polo strategico nazionale, gestito dall’omonima società, per mettere a disposizione delle PA servizi cloud di tipi IaaS (*Infrastructure as a service*), PaaS (*Platform as a service*) e SaaS (*Software as a service*), mentre un miliardo di euro è stato stanziato per tutte le attività connesse all’abilitazione e alla facilitazione di migrazione al cloud delle pubbliche amministrazioni.

30. Il d.l. n. 179/2012 definisce le modalità di attuazione dell’agenda digitale italiana, introdotta dall’articolo 47 del precedente d.l. Monti 9 febbraio 2012, n. 5 e prevede molteplici disposizioni in materia di digitalizzazione (identità digitale, dati di tipo aperto, sanità digitale, giustizia digitale, ecc.).

L'attuale formulazione dell'art. 33-*septies* stabilisce due differenti regimi per le PA centrali e per le PA locali. In entrambi i casi la norma per definire il perimetro di applicazione fa riferimento alla lista S.13 ISTAT.

In particolare, per le PA centrali che abbiano CED (Centri per l'elaborazione dati) non in linea con i regolamenti in materia³¹ si configurano tre possibili opzioni di migrazione dei loro CED e dei relativi sistemi informatici:

- 1) verso il Polo strategico nazionale (PSN);
- 2) verso altra infrastruttura propria già esistente e in possesso dei requisiti fissati dallo stesso Regolamento;
- 3) verso soluzioni cloud di fornitori esterni, purché esse siano coerenti con le specifiche tecniche, anch'esse definite nel Regolamento cloud ACN (art. 33-*septies*, comma 1, d.l. n. 179/2012).

Anche per le amministrazioni locali, intendendosi tutte quelle elencate nella lista S.13, si configurano similmente alle PA centrali tre possibili scelte per la migrazione, con la differenza che mentre le PAC devono migrare necessariamente verso una "propria" infrastruttura alternativa, viceversa le PAL possono migrare «verso altra infrastruttura già esistente in possesso dei requisiti fissati dallo stesso regolamento» (art. 33-*septies*, co. 1-*bis*, d.l. n. 179/2012). Con ciò si intende consentire alle PAL di avvalersi delle infrastrutture delle proprie società in house.

Come osservato per la legge n. 90/2024, anche in questo caso, l'analisi letterale della disposizione porterebbe a dedurre che gli enti nazionali di previdenza e assistenza, compresi INPS e INAIL, siano

fuori dall'ambito di applicazione dell'art. 33-*septies* del d.l. n. 179/2012. Benché le esclusioni e i limiti di applicazioni della disciplina siano elencati in specifici commi³², tuttavia l'art. 33-*septies* cita espressamente soltanto le PA centrali e le PA locali della lista S.13, che non includono gli enti previdenziali e assistenziali, annoverati nel relativo sottosettore.

La strategia italiana sul cloud è stata trasposta nella Regolamentazione tecnica di settore. Occorre premettere che, diversamente dalla strategia in materia di cybersicurezza rivolta tanto al settore pubblico quanto a quello privato, la strategia cloud del Governo italiano si riferisce esclusivamente alle pubbliche amministrazioni. Essa prevede la costruzione di una "casa moderna" per i dati e i servizi con più "stanze" aventi livelli crescenti di sicurezza commisurati alla tipologia di dati e servizi pubblici da ospitare.

La strategia si articola su tre direttrici, che coinvolgono:

- le singole PA per la classificazione di dati e servizi;
- i fornitori privati che erogano servizi cloud (c.d. CSP, ossia *cloud service provider*) per la qualificazione dei servizi cloud erogati alle PA;
- il PSN³³.

Di seguito si approfondiscono i principali adempimenti in capo alle PA in materia di cloud.

8.2. La classificazione dei dati e dei servizi pubblici

Per l'attuazione della strategia cloud le PA sono tenute anzitutto a classificare i propri dati e servizi in ordinari, critici o strategici sulla base degli

31. Emanati originariamente da AGID, poi emendati dall'ACN, i regolamenti sul cloud sono stati consolidati nel recente Regolamento cloud ACN.

32. Sono esclusi i CED delle PA centrali soggetti alla gestione di dati classificati secondo la normativa in materia di tutela amministrativa delle informazioni coperte da segreto di Stato e di quelle classificate nazionali (art. 33-*septies*, co. 3); sono previste inoltre le stesse limitazioni indicate dal CAD all'art. 2, co. 6, d.lgs. n. 82/2005, dove si stabilisce la disapplicazione della disciplina «limitatamente all'esercizio delle attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, polizia giudiziaria e polizia economico-finanziaria e consultazioni elettorali, nonché alle comunicazioni di emergenza e di allerta in ambito di protezione civile», ma se ne prevede espressamente l'applicazione «al processo civile, penale, amministrativo, contabile e tributario, in quanto compatibili e salvo che non sia diversamente disposto dalle disposizioni in materia di processo telematico» (art. 33-*septies*, co. 4-*quater*); sono inoltre disapplicate le norme dell'art. 33-*septies* nell'esercizio delle attività relative alla difesa e sicurezza nazionale svolte dalle infrastrutture digitali dell'amministrazione della difesa (art. 33-*septies*, co. 4-*bis*).

33. DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE–AGENZIA PER LA CYBERSICUREZZA NAZIONALE 2021.

effetti che la perdita di un dato o l'interruzione di un servizio può produrre. Ad esempio, i dati e servizi afferenti alle funzioni essenziali dello Stato saranno classificati come strategici, i dati sanitari dei cittadini saranno classificati come critici, mentre dati e servizi relativi a portali istituzionali delle amministrazioni saranno classificati come ordinari, in quanto le informazioni ivi contenute sono già note a tutti. La classificazione dei dati e servizi pubblici è un'operazione necessaria e propedeutica per la migrazione al cloud, ma anche per l'erogazione degli stessi servizi. Tant'è che se i servizi non sono preventivamente stati classificati ne è vietata l'erogazione agli utenti (art. 3, co. 6, Regolamento cloud ACN). Si tratta di una disposizione non presente nel previgente Regolamento sul cloud³⁴, con la quale si intende anche garantire l'utenza: un servizio pubblico può essere fruito solo se si è provveduto alle preventive operazioni di classificazione.

Il citato Regolamento, riprendendo il concetto di classificazione introdotto nella strategia cloud, prevede tre differenti classi per i dati e servizi delle PA:

- a) «ordinari», qualora la loro compromissione non determini i pregiudizi di cui alle seguenti lettere b) e c);
- b) «critici», se la loro compromissione può determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza pubblica e il benessere economico e sociale del Paese;
- c) «strategici», se la loro compromissione può determinare un pregiudizio alla sicurezza nazionale³⁵.

Lo stesso Regolamento disciplina nell'allegato 1 le modalità per la predisposizione dell'elenco e della classificazione dei dati e dei servizi della pubblica amministrazione, prevedendo delle semplificazioni per le PA. In particolare si stabilisce che l'ACN predisponga con cadenza almeno biennale elenchi predefiniti di dati e/o servizi, già corredati della relativa classificazione, per gruppi omogenei di amministrazioni sulla base di tre parametri: anzitutto, il rischio e l'evoluzione della minaccia di natura cibernetica, poi, la normativa e gli standard nazionali, europei e internazionali del settore, infine, i rischi per i diritti e le libertà delle persone fisiche (art. 4, co. 2 e 3 del Regolamento cloud ACN). Le PA, sulla base delle indicazioni fornite da ACN e rese disponibili sulla piattaforma digitale³⁶, stilano la propria classificazione dei loro dati e servizi (art. 5, comma 1, Regolamento cloud ACN) e provvedono a darne comunicazione all'ACN. Anche per le PA è previsto l'aggiornamento della classificazione dei dati e servizi con cadenza biennale³⁷ o comunque in presenza di una variazione nel frattempo intervenuta. L'ACN provvede alla verifica di conformità e comunica alla PA gli esiti di tale verifica, che possono concludersi con la convalida della piena conformità dell'elenco e della classificazione dei dati e dei servizi digitali, oppure con la conformità con prescrizioni o con la non convalida.

La classificazione dei dati e dei servizi, quindi, è un'operazione che la PA svolge secondo direttrici ben precisate dall'ACN, cui, in ogni caso spetta l'ultima parola. Una classificazione incauta, dove, ad esempio, servizi strategici fossero classificati come ordinari, esporrebbe potenzialmente l'amministrazione pubblica ad attacchi che potrebbero compromettere la sicurezza nazionale. Viceversa una classificazione

34. AGID, determinazione n. 628/2021, *Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione*.

35. Art. 3, co. 4, Regolamento cloud ACN.

36. Indicata in allegato 1, che a sua volta rinvia alla lettera z), invece che alla lettera u) dell'art. 1, comma 1 del Regolamento, la piattaforma digitale è accessibile dalla sezione "cloud" del sito istituzionale dell'ACN e consente tutte le operazioni (classificazione dei dati e dei servizi della pubblica amministrazione, adeguamento delle infrastrutture digitali per le pubbliche amministrazioni, delle infrastrutture dei servizi cloud per le pubbliche amministrazioni ovvero dei servizi cloud erogati da operatore pubblico, qualificazione dei servizi cloud).

37. L'art. 5, co. 1, del previgente Regolamento stabiliva che le PA presentassero per la prima volta all'ACN entro il 18 luglio 2022 la classificazione dei dati e dei servizi digitali. Cosicché da luglio 2024 le PA dovranno aggiornare la classificazione dei dati e servizi precedentemente presentata all'ACN.

dei dati eccessivamente prudente, nella quale, ad esempio, dati ordinari sono classificati come strategici, comporterebbe spese inutili, conseguenti a una protezione dei dati esagerata rispetto al rischio della loro eventuale compromissione.

8.3. I livelli minimi delle infrastrutture e dei servizi cloud

Il capo III del Regolamento cloud ACN definisce sia i livelli minimi delle infrastrutture digitali per le pubbliche amministrazioni³⁸, sia i livelli minimi delle infrastrutture che ospitano i servizi cloud destinati alle PA³⁹ (infrastrutture digitali per i servizi cloud), oltre che le caratteristiche dei servizi cloud che le PA possono acquisire. Non tutti i servizi cloud, infatti, possono essere utilizzati dalle pubbliche amministrazioni, ma solo quelli che siano rispondenti a determinati requisiti dettagliati nell'allegato 2, anche sulla base del *Framework nazionale per la cybersecurity e la data protection* (art. 6, co. 1, Regolamento cloud ACN), a dimostrazione dell'evidente stretta correlazione fra la qualità della fornitura cloud e le garanzie di sicurezza associate. L'allegato 2 del Regolamento è strutturato in più sezioni che delineano i livelli minimi di sicurezza, di capacità elaborativa, di risparmio energetico e di affidabilità delle infrastrutture necessari per ospitare dati e servizi ordinari. Oltre agli aspetti di riservatezza, affidabilità e integrità dei dati e servizi, devono essere osservati anche specifici requisiti connessi alla sostenibilità ambientale: quanto minore è il consumo energetico rispetto alla capacità elaborativa prodotta tanto minore sarà l'impatto per il pianeta⁴⁰. In particolare i dati e servizi ordinari delle PA possono utilizzare

solo infrastrutture conformi alle specifiche tecniche indicate nella sezione 2 dell'allegato 2; i dati e servizi critici, invece, possono utilizzare solo infrastrutture che garantiscano la conformità non solo alle specifiche tecniche indicate nella sezione 2 dell'allegato 2, ma anche a quelle indicate nella sezione 3. Infine i dati e servizi strategici devono utilizzare solo servizi cloud che, oltre a rispondere alle caratteristiche già richieste per i servizi critici (e quindi ordinari), rispondono anche alle caratteristiche indicate nella sezione 4 dell'allegato 2 (art. 7, Regolamento cloud ACN). Quanto più delicati, quindi, sono i dati e i servizi da proteggere, tanto più stringenti sono i requisiti richiesti alle infrastrutture che li ospitano.

Sono definite, invece, nell'allegato 3 le caratteristiche di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità e di portabilità dei servizi cloud dei quali le PA possono approvvigionarsi. In modo analogo a quanto descritto per le infrastrutture, l'allegato 3 stabilisce che:

- i dati e servizi ordinari possono utilizzare servizi cloud che rispondono ai requisiti della sezione 2;
- i dati e servizi critici possono utilizzare servizi cloud che rispondono ai requisiti delle sezioni 2 e 3;
- i dati e servizi strategici possono utilizzare servizi cloud che rispondono ai requisiti delle sezioni 2, 3 e 4 (art. 8, Regolamento cloud ACN).

8.4. La migrazione delle PA al cloud

La definizione dei livelli minimi per le infrastrutture e delle caratteristiche per i servizi cloud sono funzionali alle attività di migrazione che le PA

38. "Infrastrutture digitali per le pubbliche amministrazioni": le infrastrutture digitali tramite le quali sono erogati i servizi digitali delle amministrazioni, ivi inclusi: i CED delle PA, il PSN, le componenti di un'infrastruttura digitale di terzi a disposizione delle PA per l'erogazione di servizi cloud (es. housing) oppure finalizzati all'incremento delle prestazioni nell'erogazione in prossimità dei servizi digitali delle amministrazioni (c.d. infrastrutture di prossimità). Nello specifico, si può trattare di un singolo server o di un altro insieme di risorse di calcolo connesse, operati nell'ambito di un'infrastruttura di prossimità, generalmente situati all'interno di un data center che opera all'estremità dell'infrastruttura, e quindi fisicamente più vicini agli utenti destinatari rispetto a un nodo cloud in un data center centralizzato (art. 1, co. 1, lett. m) del Regolamento cloud ACN).

39. Cosiddette "Infrastrutture dei servizi cloud per le pubbliche amministrazioni", ossia le infrastrutture digitali per le PA fornite da un operatore di infrastrutture digitali, tramite le quali sono erogati i servizi cloud per le pubbliche amministrazioni, (art. 1, co. 1, lett. n) del Regolamento cloud ACN).

40. Tutte le misure del PNRR di ciascuno Stato membro, peraltro, richiedono il rispetto di specifici requisiti di sostenibilità ambientale, riassunti nel principio cosiddetto DNSH (*Do Not Significant Harm*), connesso alla politica del *Green deal* europeo che mira a far diventare l'Europa il primo continente a impatto climatico zero.

dovranno effettuare, in attuazione del capo IV del Regolamento. Coerentemente con quanto indicato nella strategia sul cloud, infatti, il Regolamento ribadisce che i dati e servizi delle PA migrano verso infrastrutture e servizi cloud che abbiano rispettivamente livelli di servizio e caratteristiche commisurate con la particolarità del dato e del servizio da ospitare. Infrastrutture e servizi cloud adeguati per dati e servizi strategici lo saranno anche per i dati e servizi critici ed ordinari. Come pure infrastrutture e servizi cloud adeguati per dati e servizi critici potranno ospitare anche quelli ordinari, ma non quelli strategici, perché non saranno conformi ai livelli minimi/caratteristiche indicati nella sezione 4 rispettivamente dell'allegato 2 e dell'allegato 3 al Regolamento. La migrazione al cloud, che le PA devono effettuare in attuazione del citato art. 33-*septies* del d.l. n. 179/2012, va completata entro il 30 giugno 2026 (art. 11, comma 4, Regolamento cloud ACN), data che peraltro coincide con la chiusura del PNRR. L'attività richiede, fra l'altro, la predisposizione di piani di migrazione da caricare sulla piattaforma messa a disposizione dal Dipartimento per la trasformazione digitale, alla quale accedono anche l'ACN e l'AGID per le attività di rispettiva competenza. In particolare all'AGID è assegnato un ruolo di vigilanza, verifica, controllo e monitoraggio del rispetto degli obblighi di transizione digitale. In caso di violazione di tali obblighi, l'art. 18-*bis* del CAD – introdotto come ulteriore leva a garanzia dell'attuazione del PNRR – arriva a prevedere, in caso di reiterata e grave inottemperanza da parte della PA, la nomina di un commissario *ad acta* da parte del Presidente del Consiglio dei ministri.

8.5. L'adeguamento delle infrastrutture e dei servizi, la qualificazione dei servizi cloud

Il Regolamento stabilisce 4 livelli per i requisiti di adeguamento, da AI1 a AI4, dettagliati nell'allegato 4, che sono relativi alle infrastrutture digitali per le pubbliche amministrazioni e alle infrastrutture dei servizi cloud per le pubbliche amministrazioni (art. 12). I requisiti di ciascun livello sono elaborati tenuto conto di diversi aspetti: fattori di rischio ed evoluzione della minaccia cibernetica; normativa e standard nazionali, europei e internazionali; schemi di certificazione nazionali ed europei

progressivamente adottati; migliori pratiche e linee guida di settore.

In particolare i dati e i servizi digitali classificati “ordinari” sono erogati tramite infrastrutture digitali per le pubbliche amministrazioni ovvero infrastrutture dei servizi cloud per le pubbliche amministrazioni accreditate AI1, AI2, AI3 o AI4; quelli “critici” tramite infrastrutture accreditate AI2, AI3 o AI4; mentre quelli “strategici” sono erogati tramite infrastrutture accreditate AI3 o AI4 (art. 12, co. 3). Le modalità e i termini per l'adeguamento delle infrastrutture digitali per le pubbliche amministrazioni sono disciplinati nell'articolo 13, mentre l'art. 14 del Regolamento definisce le modalità di adeguamento delle infrastrutture dei servizi cloud per le pubbliche amministrazioni.

Anche i servizi cloud per le pubbliche amministrazioni erogati da un soggetto pubblico, da società in house, ovvero, per espressa previsione normativa, da società a controllo pubblico, sono suddivisi in 4 livelli AC1, AC2, AC3, AC4, dettagliati in apposita sezione dell'allegato 4. I requisiti di ciascun livello, analogamente a quanto avviene per le infrastrutture, sono elaborati tenuto conto di diversi aspetti: fattori di rischio ed evoluzione della minaccia cibernetica; normativa e standard nazionali, europei e internazionali; schemi di certificazione nazionali ed europei progressivamente adottati; migliori pratiche e linee guida di settore. Con la stessa logica delle infrastrutture, anche per i servizi cloud, il Regolamento ha stabilito che i dati e i servizi digitali classificati “ordinari” possono essere erogati tramite servizi cloud di livello AC1, AC2, AC3 e AC4, quelli “critici” possono essere erogati tramite servizi cloud di livello AC2, AC3, AC4, mentre quelli “strategici” possono essere erogati solo tramite servizi cloud di livello AC3 e AC4 (art. 15, co. 5⁴¹).

Se i soggetti che erogano i servizi cloud sono differenti da quelli sopra menzionati, ossia soggetto pubblico, società in house, società a controllo pubblico, ma si tratta di fornitori privati, allora il Regolamento stabilisce 4 livelli di qualificazione (non di adeguamento), cloud di livello 1 (QC1), cloud di livello 2 (QC2), cloud di livello 3 (QC3), cloud di livello 4 (QC4), anche essi descritti nell'allegato 4. Con la stessa logica sopra

41. Si osserva che il comma 5 dell'art. 15 rinvia al comma 1, mentre invece il rinvio è da intendersi al comma 2 dello stesso articolo che disciplina i diversi livelli di adeguamento per i servizi cloud.

richiamata, il Regolamento dispone che i dati e i servizi digitali classificati “ordinari” possono essere erogati tramite servizi cloud accreditati QC1, QC2, QC3, QC4; quelli classificati “critici” possono essere erogati tramite servizi cloud accreditati QC2, QC3, QC4; mentre quelli “strategici” possono essere erogati tramite servizi cloud accreditati QC3 e QC4 (art. 17 del Regolamento cloud ACN). Il possesso della qualifica è sempre sottoposto a monitoraggio da parte dell'ACN, perché sulla base dell'aderenza o meno ai requisiti indicati nell'allegato 4 si gioca la sicurezza dei dati e dei servizi delle PA, che impatta la sicurezza nazionale. Le PA interessate potranno consultare il *Catalogo delle infrastrutture e dei servizi cloud per le pubbliche amministrazioni*⁴², che contiene l'elenco delle infrastrutture digitali, delle infrastrutture dei servizi cloud e dei servizi cloud, oltre che le relative informazioni descrittive compreso il livello di qualificazione ottenuto da ciascun fornitore per ognuno dei servizi cloud erogati.

9. Conclusioni

La scelta del Governo italiano di dare priorità all'innovazione della pubblica amministrazione per la ripresa e la resilienza del Paese deriva dalle raccomandazioni delle istituzioni europee, che hanno individuato proprio nella digitalizzazione dei servizi pubblici la chiave di volta per la crescita economica dell'Italia⁴³. Tali raccomandazioni hanno caratterizzato il nostro Piano nazionale di ripresa e resilienza che punta anzitutto allo sviluppo digitale dei servizi pubblici. Confrontando le scelte italiane con quelle operate, ad esempio, dal Governo francese per la definizione del proprio PNRR, emerge come la digitalizzazione e la cybersicurezza in Francia – pur rappresentando uno dei pilastri insieme alla transizione ecologica sui quali orientare gli investimenti e le riforme – non risultano misure altrettanto prioritarie. Il PNRR

italiano affronta la digitalizzazione e la cybersicurezza dei servizi pubblici nella prima componente della prima misura (p. 86 ss.) con un'allocazione iniziale complessiva di 9,75 miliardi di euro, pari a poco più del 5% delle risorse complessivamente stanziato. La versione del 2021 del PNRR (*Plan national de relance et de résilience*) francese, invece, tratta la digitalizzazione dei servizi pubblici solo nella componente 7 (p. 330 ss.) – terz'ultima delle 9 componenti in cui è articolato il PNRR – destinando complessivamente poco più di un miliardo di euro, pari a circa il 2,6% della stima iniziale del piano francese. Proporzionalmente ai finanziamenti originariamente stanziati per la realizzazione del PNRR dei due Paesi, pur nell'approssimazione del confronto qui suggerito, risulta che l'Italia dedica alla digitalizzazione della PA quasi il doppio delle risorse rispetto ai vicini cugini d'oltralpe.

Il nuovo scenario apertosi con il PNRR insieme al mutamento geopolitico hanno prodotto in capo alle amministrazioni pubbliche un aumento degli adempimenti di cybersicurezza, adempimenti destinati a crescere ulteriormente con l'imminente recepimento della direttiva NIS 2. Un carico enorme per le amministrazioni, come ad esempio quelle comunali. Al punto tale che l'Associazione Nazionale Comuni Italiani (ANCI), con riferimento al recente provvedimento in materia di cybersicurezza, l. n. 90/2024, ritiene che «pur in presenza di casi virtuosi di singole amministrazioni comunali capaci di difendersi e rispondere agli attacchi in maniera efficace, per gli enti locali» permanga «una generalizzata difficoltà ad attrezzarsi adeguatamente». Secondo ANCI fra i principali motivi ostativi all'adozione di adeguate misure di sicurezza vi sono la «carezza di risorse umane dipendenti con competenze tecniche adeguate, unita alla difficoltà a reperirne sul mercato di così specialistiche, anche a causa della bassa appetibilità, in termini retributivi, delle posizioni di lavoro all'interno dei Comuni», oltre che la «ristrettezza di risorse di

42. Curato dall'ACN e reso [disponibile sul suo sito](#).

43. Raccomandazione del Consiglio del 20 luglio 2020 sul Programma nazionale di riforma 2020 dell'Italia e che formula un parere del Consiglio sul programma di stabilità 2020 dell'Italia (2020/C 282/12), GUUE 26 agosto 2020, *Migliorare l'efficienza del sistema giudiziario e il funzionamento della pubblica amministrazione* (punto 4) e Raccomandazione del Consiglio del 9 luglio 2019 sul programma nazionale di riforma 2020 dell'Italia e che formula un parere del Consiglio sul programma di stabilità 2019 dell'Italia (2019/C 301/12), GUUE 5 settembre 2019, *Migliorare l'efficienza della pubblica amministrazione, in particolare investendo nelle competenze dei dipendenti pubblici, accelerando la digitalizzazione e aumentando l'efficienza e la qualità dei servizi pubblici locali* (punto 3).

bilancio da dedicare a interventi organizzativi e sui sistemi informativi», problemi «irrisolti, a meno dell'adozione di misure di supporto successive o in fase di decretazione attuativa»⁴⁴.

Se da un lato digitalizzazione, innovazione e sicurezza della PA costituiscono sempre più la forza propulsiva della crescita economica del Paese, d'altro canto appaiono persistere diversi vincoli alla loro concreta diffusione. Ciò nonostante, se guardiamo la pubblica amministrazione italiana con gli occhi degli anni passati, bisogna riconoscere che molti passi in avanti sono stati realizzati, come confermano i progressi dell'Italia, misurati dall'Europa (da ultimo *Digital Decade Country Report 2024: Italy*). Ad esempio l'istituzione dell'ACN. Sin da quando l'amministrazione pubblica ha avviato a partire dagli anni Ottanta la sua informatizzazione, è stata evidente la necessità di difenderla anche nella sua dimensione digitale. Benché siano state diverse le iniziative legislative e organizzative intraprese nel corso degli anni in materia di sicurezza cibernetica delle PA, era stato osservato come la loro parcellizzazione e il mancato coordinamento rendevano «assolutamente indispensabile» l'istituzione di «una unica autorità nazionale, investita del compito di provvedere in tema di sicurezza dei sistemi informativi pubblici»⁴⁵. Dal 2021 le funzioni di protezione cyber delle PA italiane e, in generale, del Paese, sono state finalmente affidate a un unico punto di riferimento in materia, l'Agenzia per la cybersicurezza nazionale, scelta che segna un deciso cambiamento⁴⁶. Le recenti direttive in materia cyber si rivolgono al vertice politico delle istituzioni pubbliche, evidenziando la consapevolezza che occorre un coinvolgimento di alto livello per l'efficacia dell'azione di contrasto alla cybercriminalità. Come osservato, infatti, i «processi di digitalizzazione, per loro natura, necessitano di una regia unitaria, poiché devono svilupparsi in modo

uniforme e l'ordinamento nazionale ed europeo si conformano a questa dinamica, anche per garantire un quadro chiaro e immediato nelle interrelazioni, che hanno carattere tecnico e politico assieme»⁴⁷. Anche perché la trasformazione digitale della pubblica amministrazione italiana e la sua cybersicurezza non rappresentano più soltanto una quota parte della trasformazione digitale del Paese, ma costituiscono il mezzo attraverso il quale si innesca il motore dell'innovazione dell'intero Paese⁴⁸.

L'attuazione delle politiche in materia di cybersicurezza delle PA, però, richiede ulteriori sforzi. Anzitutto occorre armonizzare la disciplina, che nel suo continuo mutare crea una tale incertezza da diventare potenzialmente il principale alibi alla sua disapplicazione. Mutamenti che sarebbe scorretto attribuire *tout court* alla velocità dell'evoluzione tecnologica, visto che la regolamentazione del dettaglio attuativo è opportunamente affidata alla normativa tecnica secondaria. In secondo luogo è necessario intensificare i piani formativi sulla cybersicurezza diretti specialmente alla dirigenza pubblica, doverosamente tenuta a incrementare le proprie conoscenze nel suo ruolo di cinghia di trasmissione fra le indicazioni politiche e l'azione amministrativa. Occorre poi adottare misure innovative per attrarre talenti in grado di realizzare i cambiamenti organizzativi e tecnologici attesi. La «bassa appetibilità, in termini retributivi», d'altra parte, non costituisce di per sé l'unico ostacolo, come mostrano gli studi in materia: servono, altresì, un ambiente stimolante e l'orgoglio di lavorare per il Paese, rappresentato da una classe manageriale illuminata e preparata, che l'immaginario collettivo non ancora attribuisce pienamente alle PA italiane.

Riferimenti bibliografici

44. ANCI 2024, pp. 1-2.

45. Cfr. SARZANA DI S. IPPOLITO 2010, p. 315 ss.

46. Cfr. VIOLA-DE BIASE 2023, pp. 115-121.

47. Cfr. CALZOLAIO 2024, p. 103.

48. Cfr. AGID 2023, «Il Piano Triennale per l'informatica nella Pubblica Amministrazione (di seguito Piano triennale) è uno strumento fondamentale per promuovere la trasformazione digitale del Paese attraverso quella della Pubblica Amministrazione italiana», p. 7. In tal senso la trasformazione digitale della PA diventa il mezzo attraverso il quale raggiungere la trasformazione digitale del Paese.

- ACN (2023), Relazione annuale al Parlamento 2023, 2023
- ACN (2022), Strategia nazionale di cybersicurezza 2022-2026
- AGID (2023), Piano triennale per l'informatica nella Pubblica Amministrazione (2024-2026), dicembre 2023
- ANCI (2024), Nota di lettura Legge 28 giugno 2024, n. 90 recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" pubblicata nella Gazzetta Ufficiale SG n. 153 del 2 luglio 2024, 2024
- S. CALZOLAIO (2024), Autorità indipendenti e di governo della società digitale, in F. Pizzetti, "La regolazione europea della società digitale", Giappichelli, 2024
- CIS-SAPIENZA, CINI CYBERSECURITY NATIONAL LAB (2019), Framework Nazionale per la Cybersecurity e la Data Protection, febbraio 2019
- DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE, AGENZIA PER LA CYBERSICUREZZA NAZIONALE (2021), Strategia Cloud Italia Documento sintetico di indirizzo strategico per l'implementazione e il controllo del Cloud della PA, 2021
- ISTITUTO NAZIONALE DI STATISTICA (2023), Elenco delle amministrazioni pubbliche inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196 e ss.mm. (Legge di contabilità e di finanza pubblica), settembre 2023
- E. LONGO (2024), Audizione informale per il disegno di legge in materia di «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717). Camera dei Deputati, Commissioni riunite I e II - Roma, 28 marzo 2024, in "Rivista italiana di informatica e diritto", 2024, n. 1
- C. SARZANA DI S. IPPOLITO (2010), *Informatica, internet e diritto penale*, Giuffrè, 2010
- R. VIOLA, L. DE BIASE (2023), *Il codice del futuro. La carta europea dei diritti digitali e il senso dell'innovazione*, in "Il Sole 24Ore", 24 maggio 2023



MILENA ANTONELLA RIZZI – FEDERICO SERINI

Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano

I concetti di cybersicurezza e cyberresilienza hanno fatto ingresso nell'ordinamento giuridico nonostante i dubbi sul loro significato giuridico. Si tratta infatti di formulazioni composte da concetti che, se da una parte, come nel caso della sicurezza e della resilienza, sono di difficile concettualizzazione in senso legale, dall'altra, per quanto riguarda il cyberspazio, sono perfino inediti per l'ordinamento. Il presente contributo propone una riflessione sul significato giuridico di tali termini attraverso l'interpretazione e l'indagine delle questioni ad essi sottese dalla prospettiva di diritto pubblico, ragionando sia sulla dialogica autorità-libertà propria della sicurezza, sia sui poteri del "digitale" mediante lo spettro del potere normativo.

Cybersicurezza europea e nazionale – Cyberresilienza europea e nazionale – Ordinamento e normazione tecnica

A proposed study of cybersecurity and cyberresilience concepts from a legal view between European and Italian legal systems

Cybersecurity and cyberresilience entered the legal system despite doubts about their legal meaning. These formulations are composed of concepts that, while on the one hand, as in the case of security and resilience are difficult to conceptualize in a legal sense, on the other hand, as regarding cyberspace, are even novel to the legal system. This contribution proposes a reflection on the legal meaning of these terms through an interpretation and investigation of the issues underlying them from a public law perspective analysing the authority-freedom dialogic proper to security, and the "digital" powers from the normative power view.

European and national cybersecurity – European and national cyberresilience – Legal system and technical standards

Il Prefetto Milena Antonella Rizzi è direttore del Servizio Regolazione, già Autorità e Sanzioni dell'Agenzia per la Cybersicurezza Nazionale (ACN) e dottoranda di ricerca in Studi giuspubblicistici presso l'Università di Roma Tor Vergata. Le opinioni espresse in questo contributo sono esclusivamente attribuibili all'Autrice e non riflettono la posizione dell'Agenzia per la Cybersicurezza Nazionale

Federico Serini è dottore di ricerca in Diritto pubblico, comparato e internazionale, per il curriculum di Diritto pubblico dell'economia, presso Sapienza - Università di Roma. Il 30 maggio 2024 ha concluso il percorso di dottorato difendendo una tesi dal titolo *Mercato, sicurezza e rischio informatico. Standard e certificazione dei beni ICT per esigenze di cybersicurezza nel contesto europeo e nazionale*

Questo contributo fa parte della sezione monografica *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà*, a cura di Marina Pietrangelo

SOMMARIO: 1. Premessa di studio. – 2. Il cyberspazio tra Stato, mercato e norme tecniche. – 3. Cenni su normazione tecnica e ordinamento giuridico. – 4. La normazione tecnica di cybersicurezza. – 4.1. *Il concetto giuridico di cybersicurezza europea tra sicurezza del mercato unico e sicurezza dell'umano.* – 4.2. *La cybersicurezza nazionale italiana.* – 5. Il concetto di resilienza. – 5.1. *La cyberresilienza europea e italiana.* – 6. La stabilità del cyberspazio: un bilanciamento tra continuità del servizio, libertà degli utenti e sicurezza. – 7. Considerazioni conclusive sulle cybersicurezze tra giuridico, politico e tecnico.

1. Premessa di studio

Le risorse informatiche sono un elemento essenziale per le democrazie. Tali strumenti non rappresentano solo il mezzo che consente agli individui di esprimere liberamente la propria personalità in nuove forme e modi tramite la rete¹ ma, a livello tecnico, sono anche i parametri di configurazione e funzionamento di molte infrastrutture che erogano servizi e funzioni essenziali per la società e l'economia (cc.dd. infrastrutture critiche)². Si pensi agli apparati informatici in uso presso gli operatori attivi nei settori bancario e finanziario, energetico, dei trasporti, delle comunicazioni, quello sanitario nonché quelli in dotazione presso le pubbliche amministrazioni e le varie istituzioni statali.

Questi strumenti sono ormai indispensabili sia per lo Stato in sé, sia per le sue componenti, prime fra tutte gli individui e le imprese³. Tuttavia, allo stesso tempo, sono anche responsabili di aver trasferito i rischi del cyberspazio nel mondo reale. La “rete globale” interconnessa si caratterizza infatti per essere un sistema non concepito per obbedire

a criteri di sicurezza, quanto piuttosto a quelli di libero accesso, interoperabilità e libero scambio delle informazioni. Principi questi che si scontrano oggi con le possibilità di *dual use*⁴ della rete e dei servizi informatici, tanto che alcuni autori hanno avvertito che oggi «ogni società è tanto vulnerabile quanto è vulnerabile l'informatica di cui fa uso» e pertanto «più le società sono avanzate, più sono vulnerabili»⁵.

Ciò spiega la recente introduzione dei concetti di cybersicurezza e cyberresilienza negli ordinamenti europeo e nazionale.

Si tratta di due specializzazioni, o “tipi”, di sicurezza la cui trattazione in senso giuridico sottende al fondamentale interrogativo di cosa significhi per l'ordinamento garantire “sicurezza” e “resilienza” *nel/del* “cyberspazio”. Questione di non trascurabile rilievo se si considera che i citati termini del dilemma sono caratterizzati da una obiettiva difficoltà nell'individuare una loro traduzione in termini giuridici.

Da una parte troviamo infatti la sicurezza. Nozione sfuggente, di difficile definizione, che può

1. FROSINI 2010, pp. 40-41.

2. GALLOTTI 2022.

3. DE VERGOTTINI 2021, p. 28.

4. I prodotti *dual use* sono i prodotti, inclusi software e tecnologie informatiche, che possono avere un utilizzo sia civile sia militare. Tali beni sono disciplinati dal Regolamento (UE) 2021/821, che istituisce un regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso.

5. LOSANO 2017, p. 22. Sugli effetti delle forme di connettività non solo dovute alle tecnologie ICT v. BARABÀSI 2014. Analogamente v. anche KHANNA 2016.

acquistare differenti significati in base ai diversi contesti ordinamentali e al momento storico di riferimento⁶, nonché variare in base alle diverse sensibilità, da persona a persona.

Dall'altra il cyberspazio, concetto che nasce nella letteratura fantascientifica degli anni Ottanta del secolo scorso e che ha trovato utilizzo in un primo momento nella dottrina strategico-militare, fino a fare recente ingresso nelle disposizioni legislative per mezzo del lemma "cyber", apposto a fianco di concetti più o meno noti al diritto (come in questo caso quelli di "sicurezza" e "resilienza") quale implicito riferimento a questo nuovo spazio, pur non essendo stato definito in termini giuridici⁷.

Il rapporto tra l'ordinamento giuridico e il cyberspazio è stato teorizzato da alcuni autori con l'introduzione del concetto di *cyberlaw*, branca del diritto specializzata nel cyberspazio.

Già nei primi anni Novanta del secolo scorso, nel periodo in cui si svolgeva un accanito dibattito sui profili di fattibilità, nonché di opportunità e legittimità di una disciplina giuridica del cyberspazio⁸, il giudice Frank Easterbrooks, in un discorso tenuto presso l'Università di Chicago nel 1996, fece ricorso alla metafora della "law of the horse"⁹ per argomentare la sua idea di inutilità della *cyberlaw*. In tale occasione il giudice ricordò gli insegnamenti del decano Gerhard Casper, il quale affermava che «il miglior modo per apprendere il diritto applicabile a specifici settori è quello di studiare le regole generali». In caso contrario, si andrebbe incontro ad un pericoloso rischio di diletterismo multidisciplinare che porterebbe il "cieco" – ossia lo studioso specializzato in un solo settore – ad essere un pessimo pioniere.

Condividiamo questa impostazione, valida non solo per studiare il progresso tecnologico dalla prospettiva giuridica, ma, come insegna illustre dottrina, anche per lo studio della sicurezza che non può risolversi nella mera tassonomia dei "tipi" originati dalle esigenze via via avvertite nel tempo, ma piuttosto nella riconduzione e rilettura di questi tipi all'interno della riflessione sulla sicurezza in generale¹⁰.

Pertanto, dopo una breve contestualizzazione delle questioni poste sullo sfondo (parr. 2 e 3), nel proseguo tenteremo di analizzare e ricondurre i concetti di cybersicurezza (par. 4) e cyberresilienza (par. 5) nell'alveo della sicurezza in generale. L'analisi ci darà così modo di ragionare sul rapporto tra le individuate cybersicurezze e i diritti nel cyberspazio (par. 6), e infine concluderemo la riflessione tornando sul dibattito relativo alla dimensione politica e giuridica della sicurezza in riferimento alle mutazioni apportate dall'informatizzazione (par. 7).

2. Il cyberspazio tra Stato, mercato e norme tecniche

Il dibattito sul governo del cyberspazio, ossia, sull'interesse degli Stati a regolare e controllare questo nuovo e inedito spazio che ha la caratteristica di essere un "non territorio", è un tema che può essere interpretato più in generale come una prova della sovranità degli Stati al tempo della globalizzazione¹¹. Il cyberspazio rappresenta infatti una sfida per l'esercizio dei pubblici poteri da sempre legati all'elemento materiale della territorialità¹².

Curiosa è la genesi di questa dimensione. Il cyberspazio è un fenomeno originariamente

6. ROTHSCHILD 1995.

7. Sul punto MONTI 2023B, p. 66, ove l'A. scrive che «invenzioni letterarie come il "ciberspazio" e il suo corollario "virtuale" hanno influenzato negativamente la riflessione giuridica [...] essi non sono né fictio juris (come la persona giuridica) né metafore giuridiche (come la nozione di fonti del diritto), necessarie al funzionamento del Sistema. Di conseguenza, pur mantenendo un'indubbia utilità per spiegare fenomeni sociologici, psicologici e anche economici – come appunto, il metaverso – "ciberspazio" e i suoi derivati non dovrebbero avere alcun ruolo nell'individuazione di obiettivi normativi e nella loro trasposizione in leggi e regolamenti». Più diffusamente sul punto v. anche MONTI 2023A.

8. POLLICINO-BASSINI-DE GREGORIO 2022, p. 4 ss.

9. ESTERBROOK 1996, p. 207 ss.

10. MOSCA 2021.

11. Per quanto riguarda la "sovranità digitale" v. BALDONI 2024.

12. IRTI 2006, p. 4.

pubblico, nato con il progetto Arpanet, successivamente sviluppato e diffuso per mezzo dei privati, fuori dal controllo degli Stati¹³. Difatti, l'ingresso dell'informatica nel mercato e nella società è stato un evento di scarso interesse per il potere pubblico, il quale in questo primo momento si è limitato ad intervenire con norme volte a favorire l'economia e gli investimenti in questo settore, nonché la regolazione dei meccanismi di funzionamento tecnico della rete, senza mai interessarsi di intervenire sui risvolti "politici" dello stesso¹⁴.

Dopo un primo periodo di indifferenza, la sempre maggiore rilevanza sociale ed economica di questo ambiente, appresa anche a seguito dei crescenti attacchi e malfunzionamenti dell'informatica, hanno portato i pubblici poteri a volgere l'attenzione verso questo spazio, dimostrando «non solo di [poterlo] regolamentare ma anche "iper-regolare"»¹⁵.

Tuttavia, l'elevato *expertise* richiesto nella regolazione di materie a contenuto tecnico-scientifico, nonché la mutabilità della tecnica in sé, sono i motivi per cui sempre più spesso si assiste ad una delegazione della competenza regolatoria da parte dei legislatori – attraverso i criteri del rinvio (fisso o mobile) e dell'incorporazione del contenuto di dette norme nella norma giuridica – agli enti di normalizzazione responsabili della produzione degli standard industriali.

Il dato è particolarmente significativo per quel che qui interessa. Come accennato, il cyberspazio è una dimensione che non appartiene ad alcun territorio ma che vive nei diversi elementi di cui è composto, di cui perlopiù, elementi fisici (gli hardware) e logici (i software), quali beni industriali che vengono scambiati nel mercato secondo le leggi della domanda e dell'offerta.

Da questa prospettiva, il cyberspazio può allora essere interpretato come un agglomerato di

"merci", o meglio di prodotti, processi e servizi che attengono alle tecnologie dell'informazione e della comunicazione (beni ICT) – da qui la definizione che proponiamo di "cyberspazio merceologico"¹⁶ – quale realtà in continua espansione in funzione degli sviluppi delle tecnologie informatiche che fanno ingresso nei mercati e che seguono pertanto le relative logiche e regole del mercato, nonché i relativi standard di produzione e di qualità.

Ciò è la ragione per cui il potere pubblico degli Stati in questa dimensione sembra cedere il passo alla normazione tecnica, quale strumento di regolazione che "parla" il linguaggio del mercato in quanto creata e sviluppata sulla scorta degli interessi degli stakeholder del settore.

Il tema ci porta quindi a riflettere sull'effettivo esercizio di potere nel cyberspazio attraverso lo spettro del potere normativo chiedendoci se questo risieda oggi negli Stati e nell'Unione europea o piuttosto nei privati che presenziano in questo settore, e soprattutto se la natura di questo potere sia politica o tecnica.

3. Cenni su normazione tecnica e ordinamento giuridico

Possiamo definire brevemente la normazione tecnica come quella «attività di produzione di norme atte ad individuare le caratteristiche tecniche, merceologiche e qualitative dei prodotti industriali da immettere sul mercato nonché, più recentemente, dei sistemi e processi industriali e dei servizi»¹⁷.

L'innovazione e lo sviluppo tecnologico sono da sempre legati alla normazione di tipo tecnico¹⁸. Tuttavia, se fino all'età moderna tale regolazione risultava essere condotta in modo non sistematico¹⁹, è a seguito della rivoluzione industriale che prende avvio l'attività di normazione nel senso

13. BOMBELLI 2017, p. 26; DELLA MORTE 2018, p. 27, ove l'A. precisa che l'Internet è solo una regione del cyberspazio e pertanto i due termini non sono sinonimi.

14. O'MARA 2019.

15. POLLICINO 2023, p. 415.

16. Sia concesso rinviare a SERINI 2023.

17. CAIA-ROVERSI MONACO 1995, p. 13.

18. INKSTER 2008.

19. Si trattava di standard applicativi prodotti per ogni ambito dell'esistenza umana, dall'ingegneria edile alla produzione agricola e così via, ma senza avere un parametro di uniformazione su tali regole settoriali.

moderno del termine²⁰, ossia quando si afferma l'avvertita necessità di "unificare" tali norme²¹.

Tale attività ha interessato diversi aspetti che vanno dall'uniformazione delle unità di misura, all'unificazione terminologica fino a quella dimensionale dei prodotti e delle loro componenti²². Ciò su cui concentreremo la nostra attenzione è l'evoluzione di tale normazione dal piano delle singole aziende a quello più ampio internazionale attraverso l'istituzione di appositi centri di formazione di dette norme.

La normazione tecnica nasce infatti nel contesto industriale dapprima dall'esigenza delle singole aziende di definire le caratteristiche costruttive e dimensionali dei propri prodotti come specifiche interne «custodite gelosamente», generando di conseguenza effetti di c.d. *vendor lock-in* che obbligavano i clienti a rivolgersi sempre allo stesso fabbricante²³.

In questo primo periodo, il ricorso alle norme tecniche è quindi prevalentemente orientato verso obiettivi individuali delle singole imprese. Il passaggio dall'utilizzo di tali strumenti a fini di mercato, anziché seguendo una logica produttiva strettamente individuale, è un processo che si è sviluppato gradualmente nel tempo. Tale evoluzione ha consentito di passare dall'utilizzo della normazione tecnica come strumento per guadagnare posizioni di potere nel mercato, secondo logiche di monopolio, a un ruolo chiave nella realizzazione di un mercato aperto e competitivo attraverso l'uniformazione.

È così che le attività di normazione tecnica vengono portate «fuori dagli ambiti aziendali (dove comunque permangono specifiche interne di qualità) e vengono convogliate in organismi indipendenti, a carattere settoriale o nazionale, di

cui fanno parte, oltre ad esponenti delle industrie, rappresentanti delle pubbliche amministrazioni e delle università»²⁴.

Gli enti di normazione sono soggetti, spesso di natura privata, responsabili della produzione delle norme tecniche. Operano nel multilivello e, «per motivi essenziali storici», non sono più di tre: uno per il settore elettronico, uno per il settore delle telecomunicazioni e l'altro per tutti gli altri settori²⁵.

A livello internazionale sono presenti l'*International Organization for Standardization* (ISO), l'*International Electrotechnical Commission* (IEC) e l'*International Telecommunication Union* (ITU). A livello europeo troviamo invece l'*European Committee for Standardization* (CEN), l'*European Committee for Electrotechnical Standardization* (CENELEC) e l'*European Telecommunications Standards Institute* (ETSI). In Italia gli organismi riconosciuti sono l'*Ente Nazionale Italiano di Unificazione* (UNI) e il *Comitato Elettrotecnico Italiano* (CEI).

Dal punto di vista giuridico, sebbene prenda il nome di "norme", tali strumenti non hanno natura giuridica in quanto la loro formazione non avviene per mezzo di un processo giuridico-politico, ma attraverso i ricordati alternativi centri di aggregazione di interessi non statuali – per l'appunto enti di normazione – il cui fine è quello di definire univocamente caratteristiche di prodotti, metodi e processi di produzione, nonché caratteristiche o metodi e criteri di valutazione circa la prestazione di un servizio.

Una recente dottrina ha raggruppato le diverse tipologie di norme tecniche in tre gruppi, ossia: norme originate da attori privati ma promulgate dai governi sovrani; norme originate e promulgate

20. ANDREINI 1995, p. 47.

21. A tal proposito si consideri che «[i]l termine "normazione" deriva dal latino "norma" e significa "regola". Fu poi tradotto con la parola "*standardization*" in inglese, "*normalisation*" in francese e "*Normung*" in tedesco, mentre il termine italiano "unificazione" fu coniato da Gabriele D'Annunzio, nel 1921, per indicare esattamente l'attività svolta dagli enti di normazione che cominciavano a nascere in Europa agli inizi del XX secolo, ovvero stabilire regole ed, appunto, unificare secondo un ordine riconosciuto e, come tale, accettato», cfr. UNI – ENTE NAZIONALE ITALIANO DI UNIFICAZIONE 2012.

22. ANDREINI 1995, p. 47.

23. *Ivi*, p. 48.

24. *Ibidem*.

25. ANDREINI-CAIA-ELIAS-ROVERSI MONACO 1995, p. 32.

da attori privati in seguito a delega governativa; e norme adottate da attori privati senza l'approvazione o l'applicazione governativa²⁶.

Sebbene elaborata in considerazione dei tipi di produzione delle norme tecniche negli Stati Uniti, riteniamo tale tripartizione utile anche nel nostro caso, permettendoci di distinguere norme tecniche vincolanti, norme volontarie e norme tecniche armonizzate.

Relativamente alle prime, precisiamo che le norme tecniche sono per loro stessa natura vincolanti, tuttavia nel caso in cui il loro contenuto venga riprodotto, trascritto, e materialmente recepito in un testo normativo (c.d. incorporazione) «la norma tecnica incorporata nella norma giuridica, [...] assume la stessa vigenza formale “ed entra perciò a far parte, come norma imperativa, dell'ordinamento”»²⁷.

A tal proposito precisiamo che l'ordinamento italiano, con legge 21 giugno 1986, n. 317, dando attuazione alla disciplina europea in materia di normazione e procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione, ha introdotto la c.d. “regola tecnica” definita come «una specificazione tecnica o altro requisito o una regola relativa ai servizi, comprese le disposizioni amministrative che ad esse si applicano, la cui osservanza è obbligatoria, de iure o de facto, per la commercializzazione, la prestazione di servizi, lo stabilimento di un fornitore di servizi o l'utilizzo degli stessi in uno Stato membro dell'Unione europea o in una parte importante di esso [...]»²⁸.

Le norme volontarie sono invece quelle elaborate e adottate dagli enti di normazione privati e, sebbene non siano obbligatorie, godono tuttavia di una vincolatività di fatto data dalla loro diffusa osservanza da parte degli attori economici di

settore. Considerato che queste norme, originate fuori dal diritto degli Stati, sono (volontariamente) osservate da tali stakeholder di settore, riteniamo che queste norme siano espressione di un “diritto dei privati”²⁹.

All'interno di questa categoria rientra ad esempio la «norma europea», ossia «una norma adottata da un'organizzazione europea di normazione» (il CEN, CENELEC, o ETSI prima ricordati).

Infine, le norme armonizzate sono norme esistenti nel solo ordinamento europeo e sono state introdotte sulla scorta del Regolamento (UE) 1025/2012, che le definisce come norme europee adottate sulla base di una richiesta della Commissione ai fini dell'applicazione della legislazione dell'Unione sull'armonizzazione.

Al pari delle norme volontarie, nonostante la non obbligatorietà di tali strumenti, la giurisprudenza della Corte di giustizia, ed in particolare da ultimo una pronuncia della Grande sezione³⁰, riconosce una vincolatività *de facto* di tali norme in quanto i prodotti che le rispettano beneficiano di una presunzione di conformità alle prescrizioni fondamentali relative a tali prodotti stabilite dalla pertinente legislazione dell'Unione sull'armonizzazione³¹.

Ed in particolare, nel caso di specie, la Grande sezione concludeva che, sebbene il rispetto delle norme armonizzate non sia obbligatorio, la norma prodotta dal CEN è «manifestamente obbligatoria» poiché utile come metodo di prova per dimostrare la conformità dei prodotti³².

Tra le normative tecniche e l'ordinamento giuridico sussiste una relazione. La norma tecnica acquista rilevanza per l'ordinamento giuridico ogni qualvolta questa venga “assunta” al suo interno, e tipicamente ciò avviene attraverso gli istituti dell'incorporazione e del rinvio (fisso e mobile).

26. SCHWARCZ 2002, p. 5

27. SALMONI 2002, p. 162. Sul punto v. inoltre BACHELET 1966, p. 86; LUGARESI 1995, p. 421, secondo cui con l'incorporazione «le norme tecniche assumono carattere imperativo per tutti i soggetti dell'ordinamento».

28. Art. 1, lett. f, legge 21 giugno 1986, n. 317, *Disposizioni di attuazione di disciplina europea in materia di normazione europea e procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione*.

29. CESARINI 1929.

30. CGUE, C-588/21, *Public.Resource.Org and Right to Know v Commission and Others*.

31. CGUE, C-588/21, pt. 74.

32. CGUE, C-588/21, pt. 79.

Vi è incorporazione quando il contenuto della norma tecnica viene trasposto *sic et simpliciter* all'interno di una fonte giuridica (generalmente primaria e/o secondaria), mentre il rinvio consiste nell'esplicito riferimento ad una norma tecnica puntualmente indicata (rinvio fisso o materiale), oppure nell'utilizzo di clausole generali all'interno di un disposto giuridico, come ad esempio il richiamo "alle migliori tecniche disponibili", "allo stato dell'arte" o piuttosto ai "migliori standard tecnici e di sicurezza", facenti riferimento al rispetto di normative tecniche quali presupposto di una buona pratica (rinvio mobile o formale)³³.

La norma tecnica viene così acquisita all'interno della norma giuridica, e quindi nell'ordinamento, suscitando non pochi interrogativi sulla natura di tali fonti una volta che siano state incorporate o richiamate.

Relativamente al primo caso, come anticipato, la dottrina maggioritaria è pacificamente concorde nel ritenere che la norma tecnica venga "giuridicizzata", costituendo parte integrante del disposto giuridico. Diversamente, maggiori difficoltà interpretative sono state ravvisate in relazione alla qualificazione della norma tecnica oggetto di rinvio, soprattutto se si considera che tali fonti, di natura privata, e protette da diritto d'autore, troverebbero una difficile cognizione e applicazione da parte di quei soggetti che non le abbiano acquistate.

Sul punto, alcuni autori hanno sostenuto che il «mero richiamo, in un documento ufficiale, del numero, titolo o data di applicazione della normativa» – ossia il rinvio materiale – porti alla «messa in corto circuito del diritto d'autore» poiché la norma tecnica così rinviata acquista rilevanza pubblicistica³⁴. Il dubbio sembra infatti persistere relativamente al rinvio mobile, solitamente utilizzato nei casi in cui la norma giuridica si limita a dettare la disciplina generale di una materia, per poi lasciare ampio margine ai destinatari circa

l'utilizzo delle norme tecniche utili a raggiungere il risultato "al meglio delle buone pratiche".

In conclusione, escluso quest'ultimo caso, in cui la norma tecnica conserva il suo carattere di fonte volontaria non cogente, l'incorporazione e il rinvio fisso trasformano la norma tecnica in un atto giuridico, facendole così assumere la denominazione di "norma tecnica pubblica" o "regola tecnica".

Tuttavia, come è stato precisato, il ricorso all'incorporazione e al rinvio non fanno dell'ordinamento tecnico un ordinamento giuridico, poiché i prodotti del primo acquistano forza normativa solo attraverso questo metodo di «selezione volontaria operata per il tramite della legge o di altro atto-fonte dell'ordinamento giuridico», conferendo quindi alla norma tecnica «non la qualificazione di fonte del diritto ma efficacia cogente»³⁵.

4. La normazione tecnica di cybersicurezza

La pretesa di sicurezza nel cyberspazio da parte degli Stati si scontra oggi con gli effetti derivanti dal ritardo con cui il potere pubblico ha attenzionato questa dimensione.

Non è un caso se le prime definizioni di cybersicurezza (*cybersecurity*), sicurezza informatica (*computer security*) e sicurezza delle informazioni (*information security*) hanno trovato formulazione nelle normative tecniche di settore.

Secondo la sociologia, il processo di globalizzazione ha portato ad una riarticolazione dello Stato che ha di fatto trasferito alcune sue funzioni ad attori privati³⁶, tra cui, col tempo, anche quella della sicurezza³⁷.

Dalla prospettiva giuridica ciò si è tradotto in una progressiva distinzione tra ruoli e funzioni appartenenti alla sicurezza pubblica (o primaria), che si esplicita nell'esercizio di poteri autoritativi e repressivi da parte delle pubbliche autorità, e forme di sicurezza secondaria o sussidiaria (a

33. GRECO 1999, p. 37 ss.

34. GIGANTE 1997.

35. IANNUZZI 2018, p. 78 ss.

36. SASSEN 2008.

37. ABRAHAMSEN-LEANDER 2016. Sul punto si faccia riferimento alla *Confederation of European Security Services* (CoESS), unica organizzazione riconosciuta dalla Commissione europea e attiva in un costruttivo dialogo sociale settoriale con UNI Europa, l'organizzazione europea rappresentante i sindacati dei lavoratori nei settori dei servizi, rappresentativa delle realtà private che operano nel settore dei servizi di sicurezza.

sua volta distinta in sicurezza “complementare” e “comunitaria”) ove partecipano anche soggetti privati a completamento, ausilio o integrazione della funzione di polizia³⁸.

Rispetto a questi fenomeni di “privatizzazione della sicurezza”, la normazione tecnica nei settori della sicurezza risulta tuttavia essere espressione di una ulteriore evoluzione della materia che vede il coinvolgimento di soggetti privati, che nulla hanno a che fare con la sicurezza, ma che di fatto ne sono coinvolti³⁹.

Ecco, quindi, che la norma tecnica e gli enti di normazione che le producono acquistano particolare rilevanza in questo contesto, in quanto espressione delle esigenze di questi stessi attori privati operanti perlopiù nel settore Telco⁴⁰.

Prendendo in considerazione il panorama delle norme tecniche prodotte fino ad oggi è possibile distinguere almeno tre tipologie⁴¹. Le norme di primo tipo, con il quale sono stati regolati i processi produttivi al fine di garantire determinate caratteristiche dei prodotti. Le norme di secondo tipo, che hanno trovato spazio quando la normazione tecnica ha iniziato ad interessare la progettazione e le caratteristiche prestazionali dei prodotti. Infine, con l'introduzione della famiglia di norme ISO 9000, sono state introdotte le normative di terzo tipo, volte a normare l'intero sistema di produzione attraverso la formulazione dei cc.dd. sistemi di gestione della qualità.

Proprio all'interno di quest'ultima categoria, tra gli anni Ottanta e Novanta del secolo scorso, hanno iniziato a prendere forma le prime normative tecniche sulla sicurezza dei sistemi informativi e servizi informatici (*computer security*), nonché sulla sicurezza delle informazioni (*information security*)⁴².

Per il loro significato, si faccia riferimento al bollettino dell'Agenzia statunitense competente nella gestione delle tecnologie, *National Institute*

of Standards and Technology (NIST), ove per “sicurezza informatica” si intende «la protezione fornita ad un sistema informativo allo scopo di ottenere, come obiettivo applicabile, la conservazione dell'integrità, della disponibilità e della confidenzialità delle risorse del sistema informativo stesso (inclusendo hardware, software, firmware, dati e sistemi di telecomunicazione)» (NIST SP 800-14). Mentre la norma ISO/IEC 27000:2018, per “sicurezza delle informazioni”, fa riferimento alla «preservazione della riservatezza, integrità e disponibilità delle informazioni», in qualsiasi forma esse siano rappresentate (digitale o materiale), o qualunque sia la loro modalità di trasmissione (comunicazione elettronica, corriere, ecc.).

Da ciò è possibile dedurre che il fine principale di tali normative è quello di preservare tre proprietà fondamentali delle risorse informatiche e delle informazioni affinché queste possano essere considerate sicure, spesso indicate con l'acronimo R.I.D (o C.I.A. in lingua inglese), ossia: la riservatezza (*confidentiality*), quale proprietà per cui tali risorse possono essere accedute solo da chi è stato autorizzato o ne abbia il diritto; l'integrità (*integrity*), che concerne la garanzia della correttezza, coerenza e affidabilità e quindi anche la certezza che il sistema informativo e l'informazione non siano stati alterati o modificati da soggetti non autorizzati; ed infine la disponibilità (*availability*), la proprietà secondo cui le risorse informatiche e le informazioni dovranno essere utilizzabili ed accessibili ogni qualvolta il soggetto autorizzato lo richieda.

4.1. Il concetto giuridico di cybersicurezza europea tra sicurezza del mercato unico e sicurezza dell'umano

La definizione di cybersicurezza a livello europeo è stata introdotta al culmine di un lungo processo

38. MOSCA 2012, p. 26; v. anche ANTONELLI-MATTARELLA 2022, p. 131; nonché ALIQUÒ 2023.

39. FARRAND-CARRAPICO 2018, pp. 197-217.

40. Si rinvia al documento ENISA 2012, ove si dimostra che gli standard adottati nelle norme di cybersicurezza europee per garantire la sicurezza e l'integrità delle informazioni sono fortemente basati su quelli utilizzati nel mercato europeo delle telecomunicazioni. Per quanto riguarda il coinvolgimento degli operatori Telco nella disciplina NIS sia concesso rinviare a RIZZI 2023, pp. 19-21.

41. ANDREINI 1995, p. 90 ss.

42. GALLOTTI 2022, p. 122.

che ha preso avvio con la disciplina sulla protezione delle infrastrutture critiche.

Già nel 2001 la Commissione europea adottava una Comunicazione sulla criminalità informatica ove veniva data la definizione di «sicurezza dei sistemi informatici e di rete» facendo riferimento alla «capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevedibili o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema», rinviando pertanto alle richiamate caratteristiche dell'informazione sicura.

Nel 2016 è stata emanata la Direttiva 2016/1148, anche nota come direttiva *Network and Information Security* - NIS, quale prima normativa in materia di sicurezza delle reti e dei sistemi informativi, oggi abrogata dalla Direttiva (UE) 2022/2555 (direttiva NIS II) entrata in vigore il 17 gennaio 2023 e che gli Stati membri sono tenuti a recepire entro il 18 ottobre 2024⁴³.

Nonostante la rubricazione, dall'analisi dei testi emerge come il legislatore europeo abbia inteso coniugare ancora una volta la sicurezza informatica con la protezione delle infrastrutture critiche, senza dedicare una apposita disciplina alla cybersicurezza in generale. Difatti, parte delle prescrizioni volte a «garantire un livello comune elevato di cybersicurezza nell'Unione in modo da migliorare il funzionamento del mercato interno» (art. 1) consistono perlopiù in una serie di obblighi gravanti sui soggetti individuati nella direttiva come «soggetti essenziali» e «soggetti importanti»⁴⁴, che dovranno adempierli a pena di ingenti sanzioni amministrative pecuniarie⁴⁵.

Solo con il successivo Regolamento (UE) 2019/881 (c.d. *Cybersecurity Act*), l'Unione europea è intervenuta su profili più ampi della materia, introducendo – per la prima volta all'interno di un atto normativo giuridico – la nozione di “cybersicurezza”, definita all'art. 2, n. 1, come «insieme delle attività necessarie per proteggere la rete e i sistemi

informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche».

Questa formulazione non solo introduce nell'ordinamento giuridico (europeo) un concetto prima di allora esclusivamente tecnico, ma gli conferisce anche valore sociale e politico.

Ciò può essere dedotto dal fatto che nella prima parte della definizione, il riferimento alla protezione della rete e dei sistemi informativi si sostanzia nella garanzia del poc'anzi ricordato RID delle informazioni e del supporto che le contiene, quale caratteristica fondamentale della *information* e della *computer security*, già definite nelle prime norme tecniche di settore.

Tuttavia, è nella seconda parte che riscontriamo il tratto innovativo di questa definizione, ossia il riferimento alla “sicurezza dell'umano”, inteso non solo come l'utente, la persona fisica che utilizza asset informativi e informativi, ma anche qualsiasi soggetto che anche non facendone uso può essere impattato negativamente dall'informatica o da minacce veicolate attraverso di essa.

A nostro modo di vedere, la scelta del legislatore europeo è stata quella di dirigere la cybersicurezza verso un fine pubblico di protezione delle persone fisiche (oltreché di sicurezza del mercato unico), superando lo scopo tipico delle norme tecniche di settore, solitamente dirette all'esclusiva garanzia del business delle organizzazioni che intendono osservarle e certificare la loro conformità a tali norme.

4.2. La cybersicurezza nazionale italiana

Il d.l. 14 giugno 2021, n. 82, recante *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*, ha introdotto per la prima volta nell'ordinamento italiano, la nozione di “cybersicurezza nazionale” all'art. 1, co. 1, lett. a), definendola come

l'insieme delle attività, fermi restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124, e gli obblighi derivanti da trattati internazionali, necessarie per proteggere dalle minacce informatiche reti,

43. In particolare, nella legge di delegazione europea 2023, pubblicata nella *Gazzetta Ufficiale* n. 46 del 24 febbraio 2024, all'art. 3 sono individuati i principi e i criteri direttivi per l'implementazione della nuova disciplina che dovranno ispirare l'atto di recepimento della disciplina europea.

44. Cfr. art. 3, e Allegati I e II, direttiva NIS II.

45. Cfr. Capo VII, ed in particolare art. 34 direttiva NIS II.

sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico.

Precisiamo che l'inciso relativo alla «tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico» è stato introdotto nel corso dell'esame in sede referente delle Commissioni I e IX della Camera⁴⁶, per poi essere trasposto in sede di conversione nel testo della legge 4 agosto 2021 n. 109⁴⁷.

Come per la formulazione della cybersicurezza europea, anche la definizione di cybersicurezza nazionale è frutto di un processo di composizione ove è possibile individuare due anime: quella derivante dai principi e concetti elaborati nelle normative tecniche sulla sicurezza informatica e delle

informazioni; e quella di carattere giuridico-politico, relativa alla collocazione della materia *anche* tra le attività dirette alla tutela della sicurezza e dell'interesse nazionale. Motivo per cui la citata aggiunta in sede referente ha conferito particolare rilievo alla formulazione, ma ha anche aperto a problemi interpretativi.

Come già anticipato (par. 1), il riferimento alla «sicurezza nazionale» nello «spazio cibernetico» costituisce un rinvio a due concetti su cui insistono, a loro volta, dubbi interpretativi.

Relativamente al primo, si tratta di un concetto che, sebbene sia stato oggetto di un processo di normativizzazione⁴⁸, resta tuttavia una nozione fondamentalmente politica, priva di autonomia giuridica, e tendenzialmente immune dal controllo giudiziario⁴⁹. Caratteristiche che si è tentato di superare in parte con la proposta definitoria avanzata in sede referente del d.l. in merito ad

46. Il disegno di legge in questione è stato identificato con il progressivo «Atto Camera: 3161». Nello specifico si rinvia alla sezione Emendamenti del sito della Camera, ove è possibile scorrere le diverse proposte in sede referente (relative all'art.1 vi sono state otto proposte) che hanno portato all'attuale formulazione della disposizione. Gli emendamenti apportati dal Senato in sede di conversione, Atto Senato n. 2336, hanno invece interessato gli artt. 4 e successivi.

47. Si invita alla lettura del d.l. 14 giugno 2021, n. 82, coordinato con la legge di conversione 4 agosto 2021, n. 109, recante *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*.

48. Il riferimento è agli artt. 6 e 7 della legge 3 agosto 2007, n. 124, recanti rispettivamente disciplina delle Agenzie informazioni e sicurezza esterna (AISE) e interna (AISI), ove i disposti fanno riferimento alle nozioni di «difesa dell'indipendenza, dell'integrità e della sicurezza della Repubblica» (art. 6) nonché alla «sicurezza interna della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento da ogni minaccia, da ogni attività eversiva e da ogni forma di aggressione criminale o terroristica» (art. 7), ove precisiamo che le richiamate nozioni di «sicurezza della Repubblica» e «sicurezza dello Stato» sono sinonimi di «sicurezza nazionale». In particolare, la prima è stata oggetto di discussione in sede parlamentare in occasione della riforma del sistema di *intelligence* avvenuta con la richiamata legge 124/2007, ove l'espressione sicurezza della Repubblica è stata preferita ad altre definizioni in quanto «concetto [...] più ampio rispetto a quello di «Stato», utilizzato dalla legge 801/1977, che regolava in precedenza la materia» (*Dossier del Servizio studi della Camera sulla riforma dei servizi*, n. 115, del 18 dicembre 2007). Tuttavia, l'assimilazione del compito di tutela della sicurezza nazionale (*rectius* sicurezza della Repubblica) agli apparati di *intelligence* non deve far pensare che tale funzione sia esclusivamente rimessa a tali organismi. Come osserva autorevole dottrina, tale visione porterebbe ad una «semplificazione culturale» che non tiene conto del fatto che la tutela della sicurezza nazionale interseca diverse competenze che portano l'*intelligence* a collaborare con altri attori istituzionali i quali, in una «funzione non monopolista, ma pluralista», sono rappresentati dalle forze di polizia, le forze armate, la diplomazia, fino ad estendersi, di fatto, a tutta la pubblica amministrazione. (VALENTINI 2017, p. 56 ss). Secondo alcuni autori, l'estensione del concetto alla pubblica amministrazione può essere dedotta dall'interpretazione del dovere di difesa della Patria di cui all'art. 52 Cost., quale dovere di solidarietà politica che «non si riduce alla sola difesa in armi, [come difesa dal nemico esterno] essendo ben suscettibile di adempimenti attraverso la prestazione di adeguati comportamenti di impegno sociale non armato» (URSI 2022, p. 56).

49. Così MONTI 2020.

un eventuale art. 1, co. 1, lett. a-bis al decreto, ove la sicurezza nazionale veniva definita come «il dovere del Governo di proteggere e realizzare gli interessi nazionali nel rispetto dei principi costituzionali e delle prerogative del Parlamento»⁵⁰. La proposta non ha poi trovato approvazione in sede di conversione.

Per quanto riguarda lo “spazio cibernetico” invece, oltre quanto già abbiamo tratteggiato in precedenza (par. 2), pare necessario osservare che questo concetto ha trovato definizione in alcuni documenti interni. In particolare, nel “Quadro strategico nazionale per la sicurezza dello spazio cibernetico” del 2013 ove veniva definito come

l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi. Esso dunque comprende internet, le reti di comunicazione, i sistemi su cui poggiano i processi informatici di elaborazione dati e le apparecchiature mobili dotate di connessione di rete.

Secondo alcuni autori la cybersicurezza nazionale è un concetto non completamente coincidente con quello di sicurezza nazionale, ma certamente vi rientra seppur solo relativamente ai beni e servizi di natura informatica⁵¹. Tale interpretazione ci sembra percorribile. Il riferimento è difatti all'inciso «ferm[e] restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124 [...]» che quindi distingue l'azione per fini di “cybersicurezza” da quello per la “sicurezza della Repubblica”.

Tuttavia, l'orientamento delle azioni di mera sicurezza informatica e delle informazioni «anche» ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nel cyberspazio, ci permette di concludere che la cybersicurezza, quindi

diversa dalla sicurezza nazionale, ne è comunque ricompresa e si esprime attraverso una estensione dell'azione di governo in questo settore.

Si pensi alla vicenda che ha interessato le tecnologie 5G e il settore delle Telco nel 2019, ove si è dimostrato come i poteri del Governo nell'ambito della (cyber)sicurezza nazionale non si limitino più soltanto all'apposizione del segreto di Stato⁵². Nel particolare caso citato, è stata difatti evidenziata la progressiva estensione dei poteri dell'esecutivo per motivi di sicurezza anche su beni prima di allora non ricompresi nell'ambito della sicurezza nazionale e della difesa⁵³, attraverso l'esercizio dei cc.dd. *golden powers*⁵⁴.

Tuttavia, non riteniamo di poter concludere che la cybersicurezza nazionale costituisca una *species* nel contesto delle “sicurezze” nazionali⁵⁵, piuttosto pare ragionevole sostenere, come già intuito in dottrina, che la cybersicurezza nazionale sia una componente trasversale alla difesa dello Stato e all'ordine e alla sicurezza pubblica, quale «articolazione tecnica avente natura ordinatoria e non gerarchica»⁵⁶.

Infine, il riferimento agli «obblighi derivanti da trattati internazionali», ribadisce che, come per la sicurezza in generale, tale concetto non può essere definito in sede meramente nazionale, ma deve tener conto del più ampio quadro dei diritti, doveri e libertà degli ordinamenti sovranazionali.

5. Il concetto di resilienza

Secondo le scienze sociali l'indeterminatezza della minaccia che caratterizza i tempi moderni, sarebbe riconducibile al fatto che lo sviluppo della vita associata e il crescente grado di complessità dei sistemi sociali hanno reso sempre più difficile per gli attori valutare le conseguenze dei propri

50. Vedi la proposta emendativa o.1.7.2., dell'ex deputato Giovanni Luca Aresta, nelle commissioni riunite I-IX in sede referente riferita al C. 3161 o.1.7.2., pubblicata nel *Bollettino delle Giunte e Commissioni* del 15 luglio 2021.

51. Cfr. PANSA 2019, p. 34.

52. Sul punto si rinvia a BOBBIO 2011; BRUTTI 2017, p. 193 ss. nonché SCANDONE 2008, p. 397 ss. Per una lettura aggiornata sul punto v. SCANDONE 2023, p. 269 ss.

53. VALENSISE 2020.

54. FIORENTINO 2020, p. 57.

55. Cfr. art. 6, co. 2, e art. 7, co. 2, legge 124/2007 ove è previsto che l'azione delle Agenzie di informazione e sicurezza esterna (AISE) e interna (AISI), si svolge a protezione oltre degli interessi politici e militari, anche di interessi «[...] economici, scientifici e industriali dell'Italia» quali rientranti nella sicurezza della Repubblica.

56. MONTI 2020, p. 6.

comportamenti⁵⁷, dando così vita a quella che Ulrich Beck ha definito la “società del rischio”.

Deve tuttavia osservarsi come in questo clima di incertezza, che renderebbe qualsiasi azione umana fonte di eventuali rischi/pericoli, l'azione di protezione da parte del potere pubblico potrebbe facilmente scivolare in una concezione di massima sicurezza e di difesa totale che andrebbe fortemente a limitare, se non addirittura negare, le libertà umane.

La gestione del rischio diventa quindi un tema particolarmente importante e sensibile nelle democrazie costituzionali volte a tutelare le libertà nelle società post-industriali, soprattutto in considerazione del fatto che il rischio non ha necessariamente una accezione negativa di possibile futuro danno, ma anche positiva, quale fattore che stimola l'innovazione e progresso⁵⁸.

Come per la sicurezza, anche in questo caso il principio di proporzionalità gioca un ruolo fondamentale. I sistemi di gestione del rischio si basano infatti su processi che presuppongono il calcolo del rischio quale operazione che permette di rendere l'incertezza del danno calcolabile (seppur in termini stocastici), consentendo una gestione razionalizzata della crisi *ex ante* attraverso l'adozione di adeguate decisioni secondo una determinata scala di valori e stime.

Il rischio (R) è infatti determinato dal prodotto di due variabili date dall'impatto della minaccia su un determinato bene, persona o valore (I) tenuto conto del grado della probabilità (stocastica) che tale evento si verifichi (P) entrambe calcolate secondo una prestabilita unità di misura, pertanto in formula $R = I \times P$.

L'introduzione del concetto di rischio ha quindi permesso all'uomo di procedere ad una razionalizzazione e misurazione del pericolo, venendo a creare un divario tra il «rischio tecnico», ossia il

rischio che risponde a variabili oggettive ed è quindi calcolabile, e il «rischio percepito», che invece resta una sensazione soggettiva⁵⁹.

Abbiamo deciso di argomentare sul concetto di resilienza a seguito di tale breve introduzione sul rischio poiché, diversamente dalla sicurezza tradizionale che risponde a logiche ove la lesione del bene rappresenta un fallimento per le politiche di sicurezza, la resilienza si sviluppa invece su modelli di accettazione del rischio, quindi del futuro danno, e che contemplano strumenti volti a far fronte a scenari di crisi con l'obiettivo di preservare la continuità e il funzionamento di un determinato sistema⁶⁰.

La resilienza, si concentra infatti sulla prevenzione dalle minacce e sulla minimizzazione degli effetti derivanti dalla realizzazione della minaccia (danno) con un approccio di tipo proattivo⁶¹.

Tuttavia, anche in questo caso riscontriamo l'assenza di una definizione univoca del concetto, nonostante i diffusi richiami all'interno di documenti politici e giuridici negli ultimi tempi⁶².

Si tratta infatti di una nozione a cui fanno riferimento diversi campi del sapere che vanno dalle scienze dei materiali, alla psicologia, fino all'ecologia e all'economia⁶³. Quindi la troviamo sia nelle scienze esatte (*hard science*) sia in quelle umanistiche. La distinzione ci è utile poiché migrando dalla scienza dei materiali, ove per resilienza si intende il grado di resistenza alla rottura o deformazione di un elemento (c.d. prova d'urto)⁶⁴, l'utilizzo di questo concetto in riferimento agli individui, alle comunità e alla società più in generale, ha assunto secondo alcuni autori almeno tre significati: «resilience as maintenance», ove è enfatizzato l'utilizzo della capacità di adattamento per mantenere lo *status quo*; «resilience as marginality», mirando a mantenere i cambiamenti prodotti da una crisi o

57. NOCIFORA 2010, p. 104 ss.

58. GIDDENS 2000, p. 38, ove l'A. scrive che «[...] una positiva assunzione di rischio sta alla base di quell'energia che crea la ricchezza in un'economia moderna».

59. NOCIFORA 2010, p. 107.

60. Cfr. FJÄDER 2014.

61. CASTALDO 2019.

62. Sul punto v. D'ONGHIA 2020.

63. Cfr. WALKER-COOPER 2011, ove le Autrici fanno riferimento al concetto di resilienza negli studi di Crawford Stanley Holling, nell'ambito dell'ecologia e Friedrich August von Hayek, nel campo economico.

64. Cfr. “Resilienza” in *Enciclopedia della Scienza e della Tecnica*, Treccani, 2008.

uno shock in modo marginale al fine di preservare contro cambiamenti alle strutture o alle politiche esistenti; e «resilience as renewal», con l'obiettivo di trasformare, potenzialmente rimodellare, la struttura e le politiche esistenti, facendo affidamento sulla diversificazione tra molteplici strutture e istituzioni come riserve⁶⁵.

In riferimento alle scienze sociali, in prima approssimazione, possiamo quindi osservare che la nozione abbia acquistato il senso di capacità di un "sistema" di prepararsi, adattarsi e riprendersi da perturbazioni o eventi avversi tale da conservare una condizione di normalità. Accezione positiva, che si accompagna tuttavia al "lato oscuro" del concetto di resilienza quale forma di resistenza al cambiamento e quindi all'innovazione e al progresso, o come incapacità di adattamento⁶⁶.

Dal punto di vista dei *security studies*, e in particolare dalla prospettiva della Scuola di Copenaghen, nel paradigma di resilienza il decisore politico è parzialmente sollevato dal difficile compito di scegliere quali minacce prioritizzare⁶⁷, dato che tale modello è perlopiù concentrato sulla minimizzazione degli effetti delle minacce con un approccio *all hazard*, ossia considerando tutte le forme di minacce umane, tecniche e naturali, che vanno dal terrorismo e sabotaggio ai fallimenti dei sistemi tecnici e alle catastrofi naturali.

In termini giuridici non troviamo una definizione di questo concetto che, così come il lemma "cyber", ha fatto ingresso nell'ordinamento giuridico pur trovando origine in altri campi del sapere.

Ci si potrebbe tuttavia chiedere se questo non fosse già presente nell'ordinamento vivendo in altri istituti. Relativamente all'ordinamento italiano è il caso della "sicurezza civile", secondo alcuni autori assimilabile alla resilienza in quanto è anch'essa una forma di sicurezza che si sostanzia nella gestione degli eventi di crisi⁶⁸.

Ad ogni modo si tratta di una ulteriore specializzazione della sicurezza che, a nostro modo di vedere, è riconducibile nell'azione di polizia amministrativa

definita nei primi del Novecento da Oreste Ranelletti come quella attività diretta alla sicurezza delle «cose o attività che hanno una funzione sociale [...]», ossia una funzione che «deve interessare la società, in modo da permettere a questa di raggiungere alcuni suoi scopi di conservazione o di perfezionamento, se funziona bene; e in modo da danneggiare o non soddisfare la società medesima, se funziona male», tale per cui «[l]a funzione della cosa o l'attività, quindi, viene qui tutelata come un fatto sociale, non come un diritto»⁶⁹.

I riferimenti alla difesa dell'esistenza, all'integrità e funzione delle cose «al solo fine che queste cose, malamente esistendo o funzionando, non danneggino l'ordine giuridico esistente», paiano infatti sinonimi della capacità di un "sistema" di "resistere", "adattarsi", "riprendersi" alle "perturbazioni", "shock" o "crisi" in maniera tale da preservare la sua esistenza o la sua "continuità".

5.1. La cyberresilienza europea e italiana

Diversi documenti politici e giuridici menzionano i concetti di resilienza e cyberresilienza senza tuttavia darne una definizione. Tra questi rientrano anche gli atti dell'Unione europea ove, sebbene il concetto figuri nella denominazione del testo o venga spesso richiamato all'interno dell'atto, non è possibile individuare una definizione sul punto.

Ne è conferma l'analisi dei recenti atti che compongono la legislazione europea in tema di cybersicurezza: vedi la Direttiva NIS II, il Regolamento DORA (*Digital Operational Resilience Act*) e le proposte di Regolamento *Cyber Resilience Act* e *Cyber Solidarity Act*⁷⁰.

Tuttavia, pur in assenza di elementi definitivi, è chiaro che tali misure siano volte ad aumentare i livelli di sicurezza delle infrastrutture critiche, dei servizi finanziari, dei beni ICT nonché a raggiungere il più generale obiettivo di «rafforzare le capacità nell'Unione per individuare, prepararsi e rispondere alle minacce e agli incidenti di

65. BOURDEAU 2013.

66. WILLIAMS-GRUBER-SUTCLIFFE et al. 2017, p. 756.

67. DUNN CAVELTY-ERIKSEN-SCHARTE 2023.

68. LEGA 2023, p. 371.

69. RANELLETTI 1904, p. 305.

70. Sul punto v. CHIARA-BRIGHI 2024, p. 7.

cybersicurezza»⁷¹ per il solo fine di garantire il funzionamento o, meglio, la continuità, del “sistema” mercato unico europeo.

Per quanto riguarda l'Italia, nel processo di conversione del citato d.l. n. 82/2021, oltre al riferimento alla resilienza contenuto nella definizione di “cybersicurezza nazionale”, è stata introdotta in sede referente, all'art. 1, co. 1, lett. b), anche la definizione di “Resilienza nazionale nello spazio cibernetico” che si riferisce a «le attività volte a prevenire un pregiudizio per la sicurezza nazionale come definito dall'articolo 1, comma 1, lettera f), del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131», da intendersi quindi come insieme di attività volte ad evitare un «danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale».

Diversamente dalla resilienza europea, diretta a preservare la continuità e il funzionamento delle reti per garantire a sua volta il funzionamento del mercato unico, il legislatore italiano per cyberresilienza nazionale ha inteso l'insieme di azioni volte a preservare il “continuo” funzionamento del “sistema” Stato facendo quindi riferimento alle funzioni o servizi essenziali rientranti nella disciplina sul Perimetro di Sicurezza Nazionale Cibernetica (PSNC).

Sul piano amministrativo, la cyberresilienza rientra tra gli obiettivi dell'Agenzia per la cybersicurezza nazionale (ACN) attraverso la promozione di azioni comuni dirette per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di

rilevanza strategica a tutela degli interessi nazionali nel settore⁷².

L'implicito richiamo è quindi alle citate politiche e atti di diritto derivato europei in tema di protezione delle infrastrutture critiche e di sicurezza delle connessioni nonché di cybersicurezza dei beni ICT.

Infine, ulteriore riferimento, questa volta espresso, è quello relativo alle «esercitazioni nazionali e internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese»⁷³, a cui partecipano l'ACN e il Nucleo per la cybersicurezza (NC), quest'ultimo, eventualmente, anche in qualità di promotore e coordinatore⁷⁴.

Dal breve quadro tratteggiato, relativo ad entrambe le ipotesi definitorie, emerge come la cyberresilienza, ossia la preservazione della continuità del sistema, si riferisca perlopiù ad elementi non umani, e come i cittadini o la società in generale godano solo indirettamente di tale azione.

Il tema apre alla questione della (cyber)resilienza dell'umano quale recente campo di indagine di alcune analisi dei *security studies* propense a far ricomprendere nella nozione di “sistema” non solo il dominio fisico e quello informazionale del cyberspazio, ma anche il dominio cognitivo e sociale, al fine di sviluppare modelli di cyberresilienza che tengano conto anche di elementi riconducibili all'uomo quali la capacità di comprendere e far fronte psicologicamente ad una crisi⁷⁵. Si tratta di una nuova prospettiva di studio che potrebbe certamente dirci molto sulla relazione fra rischio tecnico e rischio percepito poc'anzi richiamati.

6. La stabilità del cyberspazio: un bilanciamento tra continuità del servizio, libertà degli utenti e sicurezza

«Be conservative in what you do, be liberal in what you accept from others». Nel 1980, con questo postulato l'informatico statunitense Jon Postel, uno dei creatori di Internet, dettava il principio di

71. Art. 1, proposta Regolamento (UE) 2023/109.

72. Art. 7, co. 1, lett. a) del d.l. 82/2021.

73. Art. 7, co. 1, lett. o) del d.l. 82/2021.

74. Art. 9, co. 1, lett. c) del d.l. 82/2021.

75. DUNN CAVELTY-ERIKSEN-SCHARTE 2023.

robustezza delle reti, anche noto in informatica come legge di Postel⁷⁶.

L'enunciato è particolarmente significativo in quanto sintetizza bene l'idea che ha portato alla creazione di Internet ai suoi albori, il cui valore è tuttavia ancora attuale. Si tratta infatti di uno dei principi che regolano la progettazione della trasmissione dei dati a pacchetto, che caratterizza per l'appunto il servizio Internet come lo conosciamo oggi, prevedendo che, quando si inviano dati o si sviluppano nuovi protocolli e applicazioni per Internet, si dovrebbe farlo in modo conservativo, cioè, seguendo rigorosamente gli standard e le specifiche esistenti. Dall'altro, quando si ricevono dati o si accettano connessioni, si dovrebbe essere più flessibili e tolleranti verso eventuali errori o variazioni dai protocolli standard.

L'assunto ci è utile poiché rende evidente la natura "aperta" e vulnerabile delle reti, orientate a preservare il libero flusso delle informazioni. A livello giuridico, derivati della legge di Postel sono i due principi di libero accesso e neutralità⁷⁷. Principi che permettono non solo l'utilizzo di Internet, quale servizio universale⁷⁸, ma allo stesso tempo costituiscono anche i criteri di funzionamento dell'infrastruttura stessa.

Vi è quindi un punto di contatto tra le regole che disciplinano il funzionamento e l'esistenza

della Rete (secondo l'accezione per cui è stata pensata sin dai suoi albori), e la tutela dei diritti fondamentali in Rete⁷⁹, tra cui il diritto di accesso alla stessa.

A ben vedere secondo alcuni autori il diritto di accesso non è un diritto fondamentale a sé stante, ma piuttosto è uno strumento di esercizio di altri diritti⁸⁰. Al di là delle diverse interpretazioni, se l'accesso abbia valore meramente strumentale, o sia una libertà o un diritto sociale⁸¹, il dato certo è che la Rete è indubbiamente uno strumento che consente agli individui di esprimere liberamente la propria personalità in nuove forme e modi per mezzo di essa e dei suoi diversi servizi⁸².

La precisazione è d'obbligo poiché, come si comprenderà, parlare di sicurezza o resilienza *nel/del cyberspazio*, significa innanzitutto chiedersi in quali rapporti si pone l'esigenza di sicurezza rispetto alle libertà della Rete, e da quale punto di vista ci poniamo.

Si assiste spesso ad azioni che hanno l'effetto di rompere questo legame e frammentare la Rete, o il cyberspazio. Data l'incertezza del termine, la letteratura sul punto ha enucleato tre tipologie di frammentazione:

Technical Fragmentation: conditions in the underlying infrastructure that impede the ability of systems to fully interoperate and exchange data

76. Si rinvia alla RFC 761 (acronimo di "request of comments", si tratta di un'espressione utilizzata in telecomunicazioni e informatica indicante un documento pubblicato dalla *Internet Engineering Task Force*, che riporta informazioni specifiche riguardanti nuove ricerche, innovazioni e metodologie dell'ambito informatico o, più nello specifico, di Internet) al link: <https://www.rfc-editor.org/rfc/rfc793>.

77. Per una definizione di neutralità della rete v. la pagina AGCOM (aggiornata al 25 giugno 2024) relativa a *La neutralità della Rete* ove questo concetto è definito come quel principio per cui «l'accesso ad Internet deve essere trattato in modo non discriminatorio, indipendentemente dal contenuto, dall'applicazione, dal servizio, dal terminale, nonché dal mittente e dal destinatario» (ultimo accesso 1 agosto 2024). Per una panoramica sulla definizione del principio della neutralità della rete, si veda DE FILIPPI-BELLI 2014.

78. Su Internet come patrimonio comune dell'umanità RUOTOLO 2014, p. 556 ss.; SEGURA SERRANO 2006; SPANG-HASSEN 2006.

79. Cfr. art. 1 della Dichiarazione di Paragi adottata in seno al *World Summit on Information Society* (WSIS) nel 2003 che pone come obiettivo la costruzione di una società dell'informazione a dimensione umana, aperta e caratterizzata dalla piena condivisibilità della medesima, individuando pertanto un legame con la dimensione della tutela dei diritti umani. Sul punto v. ODDENINO 2008, p. 151 ss. Per un'ampia riflessione sul tema si rinvia al fascicolo monografico CALZOLAIO 2023.

80. CERF 2012.

81. Per una efficace panoramica sull'accesso ad Internet e le relative implicazioni nel contesto nazionale ed internazionale si rinvia a PASSAGLIA 2021.

82. Cfr. FROSINI 2010, pp. 40-41.

packets and of the Internet to function consistently at all end points.

Governmental Fragmentation: Government policies and actions that constrain or prevent certain uses of the Internet to create, distribute, or access information resources.

Commercial Fragmentation: Business practices that constrain or prevent certain uses of the Internet to create, distribute, or access information resources⁸³.

In tutte le ipotesi emerge come queste azioni possano essere perpetrate tanto da poteri pubblici quanto da attori privati. Relativamente ai primi, ne sono un esempio le pratiche di *zoning*, ossia la creazione di percorsi di rete alternativi a quello ordinario (l'Internet o cyberspazio globale) che, se portate all'eccesso, possono essere l'origine di un processo di balcanizzazione della Rete, e quindi di creazione di tante sotto-reti che hanno adottato criteri logici e di funzionamento diversi rispetto all'Internet mondo⁸⁴.

Tra i casi che invece possono essere annoverati alle azioni di frammentazione dei privati possiamo far riferimento alle pratiche di *vendor lock-in* attraverso la creazione di specifiche tecniche (standard) di prodotti e servizi ICT, che possono dare vita a vere e proprie guerre di standard per il dominio sui mercati⁸⁵, o anche essere guidate da fini e obiettivi politici estranei alle logiche di mercato⁸⁶.

Tuttavia, sono possibili azioni che interferiscono sui diritti e libertà dei soggetti interconnessi anche senza ricorrere a strumenti che hanno l'effetto di frammentare la Rete, come nel caso del filtraggio e del controllo dei contenuti.

In tutti questi casi si tratta di attività poste in essere per esigenze di sicurezza interna avvertite da singoli Paesi ma che possono incidere sul servizio universale Internet in sé, nonché anche su

soggetti che risiedono al di fuori degli Stati che attuano tali politiche di sicurezza.

Come osservato da alcuni autori in considerazione della Dichiarazione universale dei diritti umani, in particolare gli artt. 19 e 29, emerge con chiarezza che «sono i governi a determinare cosa è contro la sicurezza nazionale e l'ordine pubblico nelle rispettive società [cosicché] un combattente per la libertà agli occhi di un governo potrebbe essere considerato un terrorista agli occhi di un altro paese»⁸⁷.

Il bilanciamento tra uno strumento di libertà e globale come il servizio Internet e le ragioni di sicurezza interna degli Stati può quindi variare da ordinamento a ordinamento a seconda della forma di Stato vigente, tra soluzioni che vanno dalla netta chiusura al controllo ad altre che invece privilegiano la proporzionalità.

Tuttavia, non solo i poteri pubblici hanno rilevanza in questo contesto. Ulteriore protagonista sono anche i privati che producono beni o erogano servizi ICT i quali possono anche produrre beni e servizi sul mercato, ispirati a principi non necessariamente coincidenti con quelli dello Stato presso cui sono utilizzati. Si faccia riferimento al recente caso posto in evidenza dalla stampa internazionale secondo cui Apple avrebbe notificato a dei giornalisti indipendenti indiani e ad alcuni politici dell'opposizione che il governo indiano avrebbe cercato di violare i loro iPhone⁸⁸.

Con queste brevi considerazioni abbiamo quindi cercato di ragionare sul rapporto autorità-libertà nel cyberspazio, cercando di cogliere aspetti che non si limitano solo alle forme di controllo dei contenuti che circolano in questa dimensione, ma anche a come il rapporto autorità-libertà possa

83. DRAKE-CERF-KLEINWACHTER 2016, p. 4. Il contributo nasce dall'esigenza di chiarire l'argomento in questione al fine di facilitare il confronto in senso al *World Economic Forum's Multi-year Future of the Internet Initiative* (FII) dato che il concetto di "frammentazione" non ha univoco significato: «human rights lawyer, a trade economist and a network engineer might each give the term a special shade of meaning based on their respective priorities and experiences» (*ivi*, p. 11).

84. Cfr. ODDENINO 2008, p. 74. A tal proposito è nota la "Great Firewall" adottata dal governo cinese, sul punto v. WANG 2019.

85. SHAPIRO-VARIAN 1999.

86. Nel caso della creazione di barriere commerciali nel settore delle ICT per ragioni di sicurezza interna v. PENG 2015.

87. DRAKE-CERF-KLEINWACHTER 2016, p. 32.

88. SHIH-MENN 2023.

incidere sull'infrastruttura stessa del cyberspazio, quale realtà fortemente legata alle dinamiche politiche e di mercato (par. 2).

7. Considerazioni conclusive sulle cybersicurezze tra giuridico, politico e tecnico

Giunti al termine di questa analisi, possiamo allora tentare di ricondurre le due cybersicurezze nella più ampia riflessione sulla sicurezza in generale, quale «condizione di chi e di ciò che è esente da pericoli o tutelato da possibili pericoli», che consente ai consociati di sentirsi «liberi di agire con certezza e libertà»⁸⁹.

Certezza e libertà, che non devono solo essere il frutto di uno stato di sicurezza percepita dall'individuo, ma sono anche il prodotto di un complesso e delicato bilanciamento tra autorità e libertà ove il quando e il come la sicurezza opera limitazioni alle libertà è stabilito dalla legge, nei casi in cui la Costituzione prevede che ciò possa accadere⁹⁰.

In questi termini la sicurezza tradizionale moderna si esprime come sicurezza giuridica di ispirazione *kelseniana*.

La dottrina sul punto ha distinto due coordinate quali quelle di sicurezza ottenuta *attraverso* il diritto, quale base legittimante l'azione del potere pubblico – oggi dovremmo dire anche privato – ed allo stesso tempo anche il suo limite (sicurezza giuridica rispetto al potere); e la sicurezza giuridica riferita al diritto stesso (“sicurezza nel diritto”), intesa non solo come garanzia della certezza e conoscibilità del diritto, ma anche il rispetto della procedura di formazione della norma da parte del legislatore⁹¹.

Tuttavia, oltre all'aspetto di conformità formale dell'azione pubblica all'ordinamento, emerge anche il profilo decisionale – di ispirazione *schmittiana* – relativo alla scelta del decisore politico per motivi di sicurezza relativa non solo allo strumento più opportuno, ma anche al bilanciamento degli interessi che determinano il contenuto della decisione e, ancora prima, al “se” intervenire.

La dottrina ha già avuto modo di evidenziare, in relazione all'ordinamento italiano, come la sicurezza (nazionale) sia collocata in questo limbo tra politico e giuridico, data la carenza di una sua definizione⁹².

Relativamente alle cybersicurezze, sia il legislatore italiano sia quello europeo hanno provveduto a definire questi concetti, e in entrambe le ipotesi lo hanno fatto con un implicito rinvio alle norme tecniche di sicurezza informatica e delle informazioni.

Considerato quanto appena accennato sulla sicurezza in generale, riteniamo che l'intervento della normazione tecnica nella disciplina delle cybersicurezze rappresenti una chiara evoluzione dello schema appena tracciato, ove oltre al potere “politico” e a quello “giuridico” si aggiunge anche quello “tecnico” che non possiamo più considerare neutrale.

Come evidenziato, si tratta di regole espressione di interessi privati di cui si osserva da tempo un utilizzo anche in settori di interesse pubblico⁹³, come in questo caso quello della sicurezza.

Precisiamo tuttavia che dall'analisi delle recenti discipline europee nel settore digitale, vedi il recente *IA Act*⁹⁴, emerge come l'Unione abbia posto attenzione su un particolare tipo di norma tecnica ossia la norma armonizzata che, come anticipato (par. 3), diversamente dalle altre norme tecniche, non è creata per volere degli stakeholder privati, ma è formulata dagli enti di normazione europei (CEN, CENELEC ed ETSI) su richiesta della Commissione europea. I tre enti europei possono anche rifiutare di adempiere a detta richiesta ma, qualora accettino, sono obbligati a rispettare il contenuto e i vincoli in essa contenuti. La Commissione si riserva a tal proposito di esercitare un ampio potere di controllo su tali enti, sia durante la fase di formulazione della norma, sia in fase di approvazione della stessa.

Riteniamo che con questa tipologia di norma l'Unione europea stia cercando di veicolare – come già intuito dalla definizione di cybersicurezza

89. MOSCA 2012, p. 21.

90. AMATO 2023, p. 162.

91. PECES BARBA MARTINEZ 1993, p. 226 ss. V. anche PISTORIO 2021.

92. VALENTINI 2023, p. 60 ss., nonché VALENTINI 2017.

93. SHEN-FAURE 2021; GARCIA 2011.

94. VOLPATO 2024.

europea – la normazione tecnica verso fini pubblici perseguendo obiettivi politici.

Considerati gli orientamenti interpretativi animati da diffidenza verso il progresso tecnologico, e le allusioni a futuri scenari tecno-deterministici⁹⁵ o tecnocratici⁹⁶, ove l'umanità è passivamente relegata a subire gli effetti negativi di tali sviluppi in quanto la legge è troppo lenta per inseguire la tecnologia, riteniamo che il connubio norma giuridica e normazione tecnica costituisca certamente una via con la quale una istituzione pubblica come la Commissione europea, rappresentante interessi non solo particolari, possa regolare e guidare la tecnologia senza tuttavia arrestarne il libero sviluppo. Difatti «le norme non riguardano il *ritmo* ma la *direzione* dell'innovazione»⁹⁷.

Sorge tuttavia un problema di fondo circa la tutela delle garanzie. Sebbene a partire dalla sentenza *James Elliott Construction* del 2016 la Corte di giustizia abbia giudicato le norme armonizzate come parte integrante del diritto dell'Unione e, da ultimo, con la sentenza *Public.Resource.Org* del marzo 2024,

la Corte ne abbia riconosciuto la gratuità e piena accessibilità al pubblico, è ancora dubbia la possibilità di poter far valere i diritti eventualmente lesi da dette norme con un ricorso giurisdizionale diretto avverso una norma armonizzata.

Considerata la sicurezza come limite ai diritti e alle libertà sulla base di un delicato bilanciamento giustiziabile nei profili della proporzionalità e ragionevolezza, sorgono quindi perplessità – allo stato attuale – circa l'utilizzo di detti strumenti per la tutela di interessi pubblici. Inoltre, come è stato rilevato in recente dottrina⁹⁸, si ravvisa una certa difficoltà da parte degli enti di normazione nel collaborare per la redazione delle norme tecniche nel settore della cybersicurezza, con il pericolo che ciò possa dar vita a sovrapposizioni o inutili ripetizioni che inficiano i principi di unificazione e coerenza della normazione tecnica⁹⁹, e che di conseguenza potrebbero incidere negativamente sulla corretta realizzazione ed esecuzione di politiche di cybersicurezza e cyberresilienza dettate dalla norma giuridica.

95. Il giusfilosofo Ugo Pagallo, in PAGALLO 2014, spiega le tesi tecnodeterministe facendo cenno al noto paradosso di Zenone su Achille e la tartaruga, ove tuttavia in questo caso è la tartaruga, cioè il diritto, a non riuscire a raggiungere il piè veloce Achille, cioè la tecnologia. Difatti, le tesi tecno-deterministe assegnano al progresso tecnologico un assoluto potere incontrastabile al punto che «la corsa della tecnologia sarebbe troppo imperiosa e potente, per poter essere fermata da una semplice sentenza o editto» (*ivi*, p. 20), negando così la sussistenza di un rapporto dialettico tra diritto e tecnica. Esempio di tesi tecnodeterminista è la nota legge di Moore, la quale «a differenza delle leggi della fisica o della chimica, non è una vera e propria legge ma, piuttosto, è stata (ed è tuttora) una sorta di profezia che si auto-avvera; vale a dire una sfida, o un traguardo, che vede impegnati gli esperti nel ramo dei circuiti integrati e dei micro-processori in svariati laboratori del pianeta. [...] La morale che si deve trarre da queste riflessioni è che possiamo accogliere la legge di Moore come un elemento cruciale dell'odierna rivoluzione tecnologica e, tuttavia, respingere le tesi estreme del tecno-determinismo» (*ivi*, p. 23).

96. Come distinto dalla magistrale dottrina di Natalino Irti, in IRTI 2009, pp. 122-123, «non è arduo distinguere il tecnico dal tecnocrate: il tecnico non sceglie i fini, ma sta al servizio di fini decisi dagli altri, egli ha soltanto il potere conoscitivo dei mezzi; il tecnocrate, poiché attinge ed applica le leggi naturali dell'economia, ha il potere conoscitivo dei fini. Egli sa dove bisogna andare, e perciò rifiuta o spregia la decisione politica dei fini, i quali non sono – così argomenta – materia di disputa e di voto ma di conoscenza oggettiva e neutrale», ove per «neutralità» deve intendersi «estraneità al conflitto; e il conflitto – anche si argomenta – appartiene alla politica, e non alle leggi dell'economia, le quali, appunto come oggettive e neutrali, sono certe e incontrovertibili». In questo senso si rinvia alle ricostruzioni di Claude-Henri de Rouvroy, conte di Saint-Simon.

97. FLORIDI 2022, p. 86.

98. KAMARA 2024.

99. In particolare, il riferimento è all'ETSI che era già stata oggetto di attenzioni da parte della Commissione europea nel documento *Una strategia dell'UE in materia di normazione Definire norme globali a sostegno di un mercato unico dell'UE resiliente, verde e digitale* pubblicato dalla Commissione europea nel febbraio 2022 (COM (2022) 31, 2 febbraio 2022) in merito alla procedura decisionale delineata nello statuto dell'ente, ritenuto non equilibrato. Pare infatti che questo conferisca a determinati interessi societari un potere di voto maggiore.

Riferimenti bibliografici

- R. ABRAHAMSEN, A. LEANDER (2016), *Handbook of private security studies*, Routledge, 2016
- AGCOM (2024), *La neutralità della Rete*, aggiornata al 25 giugno 2024
- G. ALIQUÒ (2024), *Sicurezza pubblica e sicurezze private*, in “Polizia moderna”, 9 gennaio 2024
- G. AMATO (2023), *Sicurezza, fra autorità e libertà*, in M. Valentini, G. Melis, “*Pro bono communi*. Scritti in onore di Carlo Mosca”, Editoriale Scientifica, 2023
- P. ANDREINI (1995), *La normativa tecnica tra sfera pubblica e privata*, in P. Andreini, G. Caia, G. Elias, F.A. Roversi Monaco (a cura di), “La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali”, il Mulino, 1995
- P. ANDREINI, G. CAIA, G. ELIAS, F.A. ROVERSI MONACO (a cura di) (1995), *La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali*, il Mulino, 1995
- V. ANTONELLI, B.G. MATTARELLA (2022), *Carlo Mosca uomo della Costituzione*, Editoriale Scientifica, 2022
- V. BACHELET (1966), *L'attività tecnica della pubblica amministrazione*, Giuffrè, 1966
- R. BALDONI (2024), *Charting digital sovereignty. A survival playbook*, Independently published, 2024
- A.L. BARABÀSI (2014), *Linked. How everything is connected to everything else and what it means for business, science, and everyday life*, Basic books, 2014
- N. BOBBIO (2011), *Democrazia e segreto*, Einaudi, 2011
- G. BOMBELLI (2017), *Dal moderno all’“ultramoderno”? Intorno al nesso diritto-tecnica-sicurezza*, in F. Pizzolato, P. Costa (a cura di), “Sicurezza e tecnologia”, Giuffrè, 2017
- P. BOURDEAU (2013), *Resiliencism: premises and promises in securitisation research*, in “Resilience: International Policies, Practices, and Discourses”, vol. 1, 2013, n. 1
- M. BRUTTI (2017), *Arcana imperii. Sulla generalogia del segreto*, in L. Forni, T. Vettor (a cura di), “Sicurezza e libertà in tempi di terrorismo globale”, Giappichelli, 2017
- G. CAIA, F.A. ROVERSI MONACO (1995), *Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali*, in P. Andreini, G. Caia, G. Elias, F.A. Roversi Monaco (a cura di), “La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali”, il Mulino, 1995
- S. CALZOLAIO (2023), *La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, in “Rivista italiana di informatica e diritto”, 2023, n. 2
- F. CASTALDO (2019), *Dalla cyber defence alla cyber resilience dell’infrastruttura critica. Alcune implicazioni strategiche e organizzative*, in “Rivista di economia e politica dei trasporti”, 2019, n. 3
- V.G. CERF (2012), *Internet Access Is Not a Human Right*, in “The New York Times”, January 4, 2012
- O.W. CESARINI (1929), *Il diritto dei privati*, Quodlibet, 1929
- P.G. CHIARA, R. BRIGHI (2024), *La dimensione della “resilienza” nel diritto UE della cybersicurezza*, in “Ragion pratica”, 2024, n. 63
- P. DE FILIPPI, L. BELLI (2014), *Network Neutrality: An Unfinished Debate*, in P. de Filippi, L. Belli, (a cura di), “Network Neutrality: an Ongoing Regulatory Debate”, 2014
- G. DELLA MORTE (2018), *Big data e protezione internazionale dei diritti umani. Regole e conflitti*, Editoriale Scientifica, 2018

- G. DE VERGOTTINI (2021), *Sicurezza e i diritti fondamentali*, in L. Efrén Ríos Vega, L. Scaffardi, I. Spigno (a cura di), "I diritti fondamentali nell'era della *digital mass surveillance*", Editoriale Scientifica, 2021
- M.V. D'ONGHIA (2020), *Resilienza, una parola alla moda*, in "Treccani", 16 ottobre 2020
- W.J. DRAKE, V.G. CERF, W. KLEINWACHTER (2016), *Internet Fragmentation: An overview*, World Economic Forum, 2016
- M. DUNN CAVELTY, C. ERIKSEN, B. SCHARTE (2023), *Making cyber security more resilient: adding social considerations to technological fixes*, in "Journal of Risk Research", vol. 26, 2023, n. 7
- ENISA (2012), *Shortlisting network and information security standards and good practices*, 2012
- F. ESTERBROOK (1996), *Cyberspace and the Law of the Horse*, University of Chicago Legal Forum, 1996
- B. FARRAND, H. CARRAPICO (2018), *Blurring Public and Private: Cybersecurity in the Age of Regulatory Capitalism*, in O. Bures, H. Carrapico (eds.), "Security Privatization. How non-security-related Private Businesses Shape Security Governance", Springer, 2018
- C. FJÄDER (2014), *The nation-state, national security and resilience in the age of globalisation*, in "Resilience: International Policies, Practices, and Discourses", vol. 2, 2014, n. 2
- L. FIORENTINO (2020), *Verso un sistema integrato di sicurezza: dai poteri speciali al perimetro cibernetico*, in G. Della Cananea, L. Fiorentino (a cura di), "I 'poteri speciali' del Governo nei settori strategici", Editoriale Scientifica, 2020
- L. FLORIDI (2022), *Etica dell'intelligenza artificiale. Sviluppi, opportunità e sfide*, Raffaello Cortina Editore, 2022
- V. FROSINI (2010), *La democrazia nel XXI secolo*, Liberilibri, 2010
- C. GALLOTTI (2022), *Sicurezza delle informazioni. Gestione del rischio. I sistemi di gestione per la sicurezza delle informazioni. La norma ISO/IEC 27001:2022. I controlli della ISO/IEC 27002:2022*, Lulu press, 2022
- L. GARCIA (2011), *Governments, the Public Interest, and Standards Setting*, in L. DeNardis (ed.), "Opening Standards: The Global Politics of Interoperability", The MIT Press, 2011
- A. GIDDENS (2000), *Il mondo che cambia. Come la globalizzazione ridisegna la nostra vita*, il Mulino, 2000
- M. GIGANTE (1997), *Effetti giuridici nel rapporto tra tecnica e diritto: il caso delle «norme armonizzate»*, in "Rivista italiana di diritto pubblico comunitario", 1997, n. 1
- N. GRECO (1999), *Crisi del diritto, produzione normativa e democrazia degli interessi. Esemplarità della normazione tecnica in campo ambientale*, in AA.VV., "Crisi del diritto, produzione normativa e democrazia degli interessi", Edistudio, 1999
- I. KAMARA (2024), *European cybersecurity standardisation: a tale of two solitudes in view of Europe's cyber resilience, Innovation*, in "Innovation: The European Journal of Social Science Research", 2024
- P. KHANNA (2016), *Connectography. Le mappe del futuro ordine mondiale*, Fazi, 2016
- A. IANNUZZI (2018), *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Editoriale Scientifica, 2018
- I. INKSTER (ed.) (2008), *History of technology*, vol. 28, Continuum, 2008
- N. IRTI (2009), *L'ordine giuridico del mercato*, Laterza, 2009
- N. IRTI (2006), *Norma e luoghi*, Laterza, 2006
- L. LEGA (2023), *Sicurezza civile. Un sistema complesso che guarda alle crisi*, in M. Valentini, G. Melis, "Pro bono communi. Scritti in onore di Carlo Mosca", Editoriale Scientifica, 2023

- M.G. LOSANO (2017), *Guerre ibride, omicidi mirati, droni: conflitti senza frontiere e senza diritto*, in L. Forni, T. Vettor (a cura di), "Sicurezza e libertà in tempi di terrorismo globale", Giappichelli, 2017
- N. LUGARESI (1995), *Profili comparatistici della norma tecnica: l'esperienza francese dell'AFNOR*, in P. Andreini, G. Caia, G. Elias, F.A. Roversi Monaco (a cura di), "La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali", il Mulino, 1995
- A. MONTI (2023A), *Digital rights delusion: humans, machines and the technology of information*, Routledge, 2023
- A. MONTI (2023B), *Metaverso e convergenza tecnologica: aspetti (geo)politici, giuridici e regolamentari*, in G. Cassano, G. Scorza (a cura di), "Metaverso: diritti degli utenti, piattaforme digitali, privacy, diritto d'autore, profili penali, blockchain e NFT", Pacini Giuridica, 2023
- A. MONTI (2020), *Ordine pubblico, sicurezza nazionale e sicurezza cibernetica: una prospettiva di sistema*, in "1° Quaderno Speciale CASD – Scenari globali e interessi nazionali: pandemia, continuità, cambiamento", 18 dicembre 2020
- C. MOSCA (2021), *La sicurezza. Valori, modelli e prassi istituzionali*, Editoriale Scientifica, 2021
- C. MOSCA (2012), *La sicurezza come diritto di libertà. Teoria generale delle politiche della sicurezza*, Cedam, 2012
- E. NOCIFORA (2010), *Sociologia della sicurezza, rischio e legalità democratica*, in AA.VV., "Sicurezza e democrazia", Scriptaweb, 2010
- M. O'MARA (2019), *The Code: Silicon Valley and the Remaking of America*, Penguin Press, 2019
- A. ODDENINO (2008), *La governance di Internet fra autoregolazione, sovranità statale e diritto internazionale*, Giappichelli, 2008
- U. PAGALLO (2014), *Il diritto nell'età dell'informazione: il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, Giappichelli, 2014
- A. PANSÀ (2019), *La sicurezza nazionale. Innovazione e nuovi limiti*, in "Gnosis", 2019, n. 1
- P. PASSAGLIA (2021), *La problematica definizione dell'accesso a Internet e le sue ricadute su esclusioni sociali e potenziali discriminazioni*, in "MediaLaws. Rivista di Diritto dei Media", 2021, n. 3
- G. PECES BARBA MARTINEZ (1993), *Teoria dei diritti fondamentali*, Giuffrè, 1993
- S. PENG (2015), *Standards as a Means to Technological Leadership? China's ICT Standards in the Context of the International Economic Order*, in L. Toohey, C.B. Picker, J. Greenacre (eds.), "China in the International Economic Order: New Directions and Changing Paradigms", Cambridge University Press, 2015
- G. PISTORIO (2021), *La sicurezza giuridica: profili attuali di un problema antico*, Editoriale Scientifica, 2021
- O. POLLICINO (2023), *Potere digitale*, Estratto da "I Tematici, V-2023 – Potere e Costituzione", in "Enciclopedia del diritto", 2023
- O. POLLICINO, M. BASSINI, G. DE GREGORIO (2022), *Internet Law and Protection of Fundamental Rights*, Bocconi University Press, 2022
- O. RANELLETTI (1904), *La polizia di sicurezza*, in V.E. Orlando (a cura di), "Primo trattato completo di diritto amministrativo italiano", vol. IV, Società Editrice Libreria, 1904
- M.A. RIZZI (2023), *L'evoluzione del panorama regolamentare cyber e l'avvento della Direttiva NIS2 nel settore delle telecomunicazioni*, in "Cyber Magazine – Cyber Think Tank Assintel", sett-ott. 2023
- E. ROTHSCHILD (1995), *What is security?*, in "Daedalus", vol. 124, 1995, n. 3

- G.M. RUOTOLO (2014), *Internet (diritto internazionale)*, in “Enciclopedia del diritto”, Annali VII, Giuffrè, 2014
- F. SALMONI (2001), *Le norme tecniche*, Giuffrè, 2001
- S. SASSEN (2008), *Territory, Authority, Rights: From Medieval to Global Assemblages*, Princeton University Press, 2008
- G. SCANDONE (2023), *Il segreto di Stato e la difesa della Repubblica. L'insegnamento dei recenti eventi internazionali*, in M. Valentini, G. Melis, “Pro bono communi. Scritti in onore di Carlo Mosca”, Editoriale Scientifica, 2023
- G. SCANDONE (2008), *Il segreto di Stato*, in C. Mosca, G. Scandone, S. Gambacurta, M. Valentini, “I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)”, Giuffrè, 2008
- S.L. SCHWARCZ (2002), *Private Ordering*, in “Northwestern University Law Review”, vol. 97, 2002, n. 1
- A. SEGURA SERRANO (2006), *Internet Regulation and the Role of International Law*, in “Max Planck Yearbook of United Nations Law”, vol. 10, 2006
- F. SERINI (2023), *La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana*, in “Rivista italiana di informatica e diritto”, 2023, n. 2
- C. SHAPIRO, H.R. VARIAN (1999), *The Art of Standards Wars*, in “California Management Review”, vol. 41, 1999, n. 2
- Y. SHEN, M. FAURE (2021), *Private standards for the public interest? Evidence from environmental standardization in China*, in “Review of European, Comparative and International Environmental Law”, vol. 30, 2021, n. 3
- G. SHIH, J. MENN (2023), *India targets Apple over its phone hacking notifications*, in “The Washington Post”, December 27, 2023
- H. SPANG-HASSEN (2006), *Public International Computer Network Law Issues*, Djoef Publishing, 2006
- UNI – ENTE NAZIONALE ITALIANO DI UNIFICAZIONE (2012), *Le regole del gioco*, UNI, 2012
- R. URSI (2022), *La sicurezza pubblica*, il Mulino, 2022
- B. VALENSISE (2020), *I settori strategici dopo la Riforma*, in G. Della Cananea, L. Fiorentino (a cura di), “I ‘poteri speciali’ del Governo nei settori strategici”, Editoriale Scientifica, 2020
- M. VALENTINI (2023), *Sicurezza della Repubblica tra politico e giuridico* (prima parte), in “Amministrazione Pubblica. Rivista di Cultura Istituzionale dei Funzionari dell'Amministrazione Civile dell'Interno”, 2023, n. 113
- M. VALENTINI (2017), *Sicurezza della Repubblica e democrazia costituzionale. Teoria generale e strategia di sicurezza nazionale*, Editoriale Scientifica, 2017
- A. VOLPATO (2024), *Il ruolo delle norme armonizzate nell'attuazione del regolamento sull'intelligenza artificiale*, in “Quaderni AISDUE”, fasc. speciale, 2024, n. 2
- J. WALKER, M. COOPER (2011), *Genealogies of Resilience: From Systems Ecology to the Political Economy of Crisis Adaptation*, in “Security Dialogue”, vol. 42, 2011, n. 2
- X. WANG (2019), *The Great Firewall of China and Its Implications for Political Information Systems*, 2019
- T.A. WILLIAMS, D.A. GRUBER, K.M. SUTCLIFFE et al. (2017), *Organizational response to adversity: Fusing crisis management and resilience research streams*, in “Academy of Management Annals”, vol. 11, 2017, n. 2

Sezione monografica

EMFA under the spotlight: towards a common regulatory framework
to foster media pluralism? - Part 1

a cura di
Elda Brogi



RIVISTA ITALIANA DI
INFORMATICA E DIRITTO

PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0198 • articolo non sottoposto a peer review • pubblicato in anteprima il 19 dic. 2024
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale 

ELDA BROGI

EMFA under the spotlight: towards a common regulatory framework to foster media pluralism?

Introduction

The Author is EUI Part-Time Professor and Scientific Coordinator of the Centre for Media Pluralism and Media Freedom

This paper is part of the monographic section *EMFA under the spotlight: towards a common regulatory framework to foster media pluralism?* edited by Elda Brogi

In 2024, the European Union adopted the European Media Freedom Act (Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024). This regulation establishes a unified framework for media services within the internal market and revises Directive 2010/13/EU, the Audio-visual Media Services Directive. The act's adoption represents a notable achievement of the EU, following years of debate concerning the EU's authority to legislate over media freedom and pluralism. Although the European Union (and previously the European Community) has always acknowledged the importance of media pluralism in safeguarding democratic values and ensuring the free flow of information – as shown, for instance, by Article 11 of the European Charter of Fundamental Rights and its reference to the European Convention on Human Rights – the political and legal debate on the attribution of competences between the EU and its Member States on this matter has hindered the progress towards harmonised rules to support media freedom and media pluralism on a wider European level.

The adoption of the EMFA is justified under article 114 TFEU, commonly used as a legal basis for harmonizing laws across the EU to improve the functioning of the internal market. In the case of the EMFA, Article 114 addresses the fragmentation of media regulation across Member States that could impede the free flow of media services and the undermine of media pluralism within the EU. This choice is currently being challenged before the Court of Justice of the European Union by a member state, Hungary, which argues that divergences between national rules do not, in themselves, justify recourse to Article 114 TFEU, alongside the use of a regulation instead of a directive¹.

Historically, political discussions around EU-level legislation on media pluralism have been driven by the aim of preventing the capture and concentration of media ownership, particularly in certain countries. However, it must be acknowledged that the scope of the European Media Freedom Act extends beyond this objective. It represents a first step in reaffirming the role of media in the internal market and the centrality of media as essential elements of a democratic society, especially within the context of an evolving media market affected by the rise of online platforms. The EMFA makes a first attempt to, at least partially, tackle the increasing imbalance in market and opinion power between media and very large online platforms.

Several policies affecting media pluralism have already been introduced to indirectly address this imbalance. Examples include various global initiatives aimed at safeguarding news content through copyright protections in the digital age, such as in Australia and in the EU itself, policies that prioritize public-interest content, and specific taxation measures for digital services. On top of these measures, the rapid rise of very large online platforms, the cross-border nature of online media, and the threats posed by disinformation have already forced the EU to enact several legislative and policy measures that affect media and media pluralism through horizontal regulatory approaches. These include regulations on digital platforms, digital markets, the use of AI. While these measures indirectly touch upon media pluralism, they do not provide a comprehensive, specific approach to addressing the core challenges to plurality and independence faced by the media in a democratic society. Challenges that the EMFA, in turn, strives to achieve.

1. Case C-486/24: Action brought on 10 July 2024 – *Hungary v European Parliament and Council of the European Union*, OJ C, C/2024/5088, 26 August 2024.

For example, the adoption of the Digital Services Act² demonstrates the EU's willingness to concretely tackle aspects related to media freedom and media pluralism insofar as VLOPs and VLOSEs are concerned, but it does so in a way that does not directly protect them. Articles 34 and 35 of the DSA state that risks to "freedom and pluralism of the media, enshrined in Article 11 of the Charter" should be regularly assessed by VLOPs and VLOSEs, and that measures should be deployed to mitigate such risks. How platforms will interpret these norms remains to be seen, and in the end, these measures will work to mitigate risks rather than to safeguard rights. Some concerns, therefore, arise from the fact that VLOPs (usually large technology companies from outside the EU) are tasked, under a duty of care, (or their compliance auditors in an *ex post* assessment) with defining, interpreting and implementing measures to mitigate risks to media pluralism. This effectively grants them the authority to potentially shape the scope and quality of online public discourse.

If freedom and pluralism in the media are still essential to democratic societies, providing a platform for the exchange of diverse ideas, facilitating public discussions, and enabling citizens to make informed decisions, it is therefore welcome that an ad hoc "media freedom act" exists, as it attempts to define some correctives to the "platformisation" of fundamental rights.

The European Media Freedom Act touches upon various components of a media policy, in line with a comprehensive perspective that goes beyond assessing market concentration as the main proxy for the level of plurality in a given media market. This monographic section aims to contribute to the discussion on the interpretation of several EMFA provisions and themes, and to explore how this legislation connects and interacts with other European legislation in the digital sector.

Regarding the specific contributions, the monographic section opens with *Quale nozione di pluralismo nell'EMFA?* an article by Ottavio Grandinetti, who analyses the definition of media pluralism provided by the EMFA. He finds that it entails elements of both "external pluralism" and "internal pluralism", with the caveat that «obligations to provide "impartial, objective, balanced" information, if placed in the wrong hands, can lead to outcomes contrary to the intended goals of regulations aimed at protecting pluralism». As for new challenges to media pluralism, such as disinformation and content prioritization, the EMFA's responses lie in guaranteeing the editorial independence and integrity of media service providers, introducing rules for the personalization of content offerings, and reaffirming the prominence of media services of general interest.

Alongside this analysis of the notion of media pluralism in the EMFA, the contribution of Antonio Manganelli and Maria Luce Mariniello (*La valutazione delle concentrazioni per la tutela del pluralismo informativo*) explores the EMFA measures that tackle market concentrations with a significant impact on media pluralism and editorial independence. The EMFA foresees each member state will enact harmonised disciplines for the control of concentrations in the media markets – the so-called Media Plurality Test. This discipline entails both substantive and procedural elements. The authors suggest that the Italian experience, stemming from the implementation of Article 51 TUSMA and the AGCOM guidelines aimed at assessing the existence of significant market power positions that may harm media pluralism, could serve as a reference model for the European Commission's future guidelines on the market plurality test required by the EMFA. The authors argue that the Italian TUSMA appears substantially aligned with the EMFA's provisions.

In her article, *From Rhetoric to Regulation: EMFA and Media Concentration in the Digital Age*, Tanja Kersevan, explores how media concentration is addressed across EU member states, with a particular focus on two small EU countries, Croatia and Slovenia, where outdated laws and insufficient data for assessing media pluralism pose significant challenges for effective and harmonized implementation of EMFA provisions. In the absence of and comprehensive guidelines and coordinated efforts to achieve

2. [Regulation \(EU\) 2022/2065](#) of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27 October 2022, pp. 1-102.

consistent enforcement across Member States, the regulation may fall short in addressing risks to media pluralism, especially within the fast-changing digital landscape.

As mentioned above, public service media is included in the EMFA. In *Safeguards for the independent functioning of public service media providers. The legal position of domestic legislation that is not in compliance with Article 5 EMFA*, Enrico Albanesi examines Article 5 of the EMFA on guarantees for the independent functioning of public service media providers and the legal status of domestic legislation that is not in compliance with Article 5. The analysis focuses on the legal situation of national legislation within Member States that, by the date of the article's application (August 8, 2025), does not comply with the provisions of Article 5.

In his contribution, *The missing piece in the DSA puzzle? Article 18 of the EMFA and the media privilege* Matteo Monti delves into the heated debate on Articles 18 of EMFA, which introduces the concept of “media privilege” within the content moderation framework established by the Digital Services Act. Monti's discussion highlights several key aspects. The media privilege mechanisms grant eligible media entities specific rights on digital platforms, such as advance notice of content removal and priority review in complaint processes. The article explores the operativity of the privilege and its interface with the DSA provisions; and the transparency of its application, including the role of the Board under Article 19 of the EMFA. Challenges in the implementation and criticisms, particularly concern that disinformation agents might misuse these privileges. Monti concludes by underscoring that the media privilege provisions are designed to reaffirm the importance of professional journalism in the digital era, while also stressing the need for robust safeguards to prevent potential abuse.

Building on similar reflections, Liliana Ciliberti in *DSA e EMFA: speciale responsabilità delle piattaforme online e tutela della libertà dei media*, argues that the margin of discretion under DSA granted to very large online platforms in handling media services is excessively broad. This broad discretion raises concerns not alleviated by the so-called media privilege in the EMFA, which obliges platforms to engage in prior dialogue with media service publishers before applying any restrictions, a privilege subject to significant exceptions. Ciliberti contends that strict interpretation of these exceptions is necessary. Moreover, she calls for swift intervention by national and European institutions to clarify the limits of platform actions toward media service publishers, to prevent the delegation of public powers to platforms that the new regulatory framework appears to endorse.

One of the standout provisions of the EMFA is its focus on ownership transparency (Article 6). Media providers are required to disclose their ownership structures, increasing accountability. This measure aims to build trust with audiences while addressing concerns over media concentration. However, implementing these measures may pose challenges to governments and society at large, as analysed by Danielle Borges in *Media ownership transparency and the European Media Freedom Act: how did the EU get there?*

In the next issue of RIID, the first of 2025, another monographic section will be dedicated to further examining additional themes related to the EMFA, ensuring a comprehensive analysis of this pivotal regulation and its impact on the media landscape.

Riferimenti bibliografici

- E. BROGI, D. BORGES, R. CARLINI et al. (2023), *The European Media Freedom Act: media freedom, freedom of expression and pluralism*, European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, Study PE 747.930, 2023
- M.D. COLE, C. ETTELDORF (2024), *The European Media Freedom Act unpacked*, European Audiovisual Observatory, 2024
- M.D. COLE, C. ETTELDORF (2023), *Research for CULT Committee – European Media Freedom Act - Background Analysis*, European Parliament, Policy Department for Structural and Cohesion Policies, 2023
- F. PAOLUCCI (2024), *The European Media Freedom Act: (another) new chapter in the digital regulation saga*, in “Diritti Comparati”, 2024



OTTAVIO GRANDINETTI

Quale nozione di pluralismo nell'EMFA?

L'articolo si propone, attraverso l'analisi del regolamento (UE) 2024/1083, da un lato di verificare quale nozione di pluralismo abbia tenuto presente il legislatore europeo nell'EMFA (*European Media Freedom Act*) e, dall'altro lato, di individuare le risposte che il legislatore europeo ha dato alle c.d. nuove sfide del pluralismo informativo. La risposta al primo tema è "aperta", in considerazione della possibilità di fornire almeno due diverse letture alle previsioni dell'EMFA: una, più riduttiva (e, forse, più realistica), in base alla quale l'EMFA, per questi aspetti, sarebbe più simile ad una direttiva di armonizzazione (minima) che ad un regolamento; un'altra, meno riduttiva, in base alla quale il legislatore UE avrebbe individuato – quantomeno di default – il pluralismo interno come forma da applicare certamente ai media di servizio pubblico ed il pluralismo esterno a quelli non di servizio pubblico. Con riferimento alle nuove sfide del pluralismo, come la disinformazione e la prioritizzazione dei contenuti, le risposte dell'EMFA sembrano rintracciarsi, rispettivamente, nella garanzia dell'indipendenza ed integrità editoriale dei fornitori di servizi di media e nell'introduzione di regole di personalizzazione dell'offerta nonché nella conferma della c.d. *prominence* (debito rilievo) dei servizi di media di interesse generale.

*EMFA – Pluralismo informativo – Media di servizio pubblico – Stampa – Disinformazione
Prioritarizzazione algoritmica dei contenuti – Prominence*

What notion of pluralism in EMFA?

Through an analysis of the regulation (UE) 2024/1083, the article aims, on the one hand, to identify the concept of media pluralism that the European legislator has in mind in the EMFA (*European Media Freedom Act*) and, on the other hand, to identify the responses that the European legislator has made to the so-called new challenges of media pluralism. The answer to the first question is 'open', given the possibility of at least two different readings of the EMFA provisions: one, more reductive (and perhaps more realistic), according to which EMFA would be more like a (minimum) harmonisation directive than a regulation in these respects; another, less reductive, according to which the EU legislator would have identified – at least by default – internal pluralism as the form that should certainly be applied to public service media and external pluralism to non-public service media. With regard to the new challenges of pluralism, such as disinformation and the prioritisation of content, the EMFA's answers seem to lie in guaranteeing the editorial independence and integrity of media service providers and in introducing adaptation rules or confirming the so-called *prominence* of general interest media services.

*EMFA – Media pluralism – Public service media – Press – Disinformation
Algorithmic prioritisation of content – Prominence*

L'Autore è professore a contratto di Diritto dell'informazione presso l'Università degli Studi di Napoli Suor Orsola Benincasa e avvocato

Questo contributo fa parte della sezione monografica *EMFA under the spotlight: towards a common regulatory framework to foster media pluralism?* a cura di Elda Brogi

SOMMARIO: 1. Premessa. – 2. Alcune precisazioni sulla nozione di pluralismo. – 3. Le c.d. nuove sfide al pluralismo informativo. – 4. Alcune considerazioni generali su EMFA e pluralismo. – 5. Analisi delle previsioni più rilevanti riguardo al pluralismo. – 6. L'EMFA e le risposte ad alcune delle c.d. nuove sfide al pluralismo. – 7. Considerazioni conclusive.

1. Premessa

Nel Regolamento (UE) 2024/1083 in commento il legislatore europeo ha affrontato direttamente, come mai fatto in passato, il problema del pluralismo informativo, che in precedenti interventi normativi relativi al settore dei media audiovisivi, pur presente, era risultato meno esplicitamente centrale, anche a causa della dubbia base normativa di un intervento dell'Unione in tale materia¹.

Poiché come si dirà più ampiamente subito appresso – nonostante il termine pluralismo sia entrato ormai da tempo nel lessico degli studiosi, delle Corti e dei legislatori – deve registrarsi una qualche persistente incertezza in merito all'effettiva portata attribuita a questo termine², è sembrato del tutto naturale chiedersi quale nozione di pluralismo (ed eventualmente quali delle sue varie “declinazioni”) abbia tenuto presente l'EMFA, per quanto sia possibile evincere dai considerando e dagli articoli nonché dall'analisi complessiva dell'atto normativo.

Né sarebbe condivisibile liquidare il tema limitandosi a ricordare che, in base al principio di

attribuzione, la competenza a disciplinare il pluralismo sta in capo agli Stati membri, visto che – come si vedrà – proprio in occasione dell'EMFA il legislatore europeo si è mostrato disponibile a “forzare” le interpretazioni più restrittive, come, ad esempio, nel caso delle garanzie richieste per l'indipendenza dei media di servizio pubblico³.

2. Alcune precisazioni sulla nozione di pluralismo

In ottica molto generale e guardando al risultato finale che dovrebbe assicurare un sistema dei media pluralistico, può certamente concordarsi con la definizione secondo cui il pluralismo dovrebbe assicurare la massima diffusione di idee possibile e, dunque, prevenire il rischio che i cittadini siano esposti ad un ventaglio di opinioni troppo ristretto⁴.

Definizioni un po' meno generali sottolineano peraltro che «il pluralismo può dirsi raggiunto quando ci sono una *molteplicità di media* autonomi ed indipendenti a livello nazionale, regionale e locale, che assicurino una *varietà* di contenuti che riflettono *diverse visioni* culturali e politiche»⁵.

1. In argomento, si v. MASTROIANNI 2022, pp. IX-XXIII. Riguardo ad un apparente cambio di passo dell'Unione sulla regolazione dei media si v. pure HOLTZ-BACHA 2024.

2. BROGI-BORGES-CARLINI et al. 2023, p. 11 ss.; NJAKAS et al. 2018, p. 20.

3. A titolo esemplificativo, si v. sin d'ora le severe critiche svolte da COLE-ETTELDORF 2023, p. 17, riguardo all'interpretazione del c.d. Protocollo di Amsterdam fornita nell'*Explanatory Memorandum* della proposta di EMFA, nel senso che il medesimo Protocollo in realtà confermerebbe la “implicita” rilevanza dei media di servizio pubblico nell'ambito del mercato unico e, quindi, legittimerebbe l'intervento dell'Ue (anziché ostacolarlo).

4. In quest'ultimo senso, ad es., OFCOM 2015, p. 6.

5. EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW, *Opinion on Italian Laws*, 2005 (corsivi aggiunti); si tratta della Commissione di Venezia, organo consultivo del Consiglio d'Europa sulle materie costituzionali.

Da questa più dettagliata definizione emerge abbastanza chiaramente che l'obiettivo del pluralismo (*media pluralism*) richiede sia la pluralità di media autonomi ed indipendenti, sia la diversità dei contenuti.

Con il primo concetto si individua un certo assetto *strutturale* del settore dei media (la necessaria presenza di più operatori indipendenti), ossia quello che viene solitamente definito il pluralismo esterno (*media plurality* o *structural pluralism*).

Con il secondo concetto (in genere espresso con il termine *diversity*) si può fare riferimento ad almeno due aspetti, non del tutto sovrapponibili: l'effettiva diversità dei contenuti realizzata o all'interno di uno stesso medium (pluralismo interno o *internal pluralism*) o perlomeno in ciascun settore del complessivo sistema dei media, oppure la presenza di differenti tipologie di media (ad es., pubblici o privati e, in quest'ultimo ambito, nazionali o locali, profit o non profit, ecc.); di diverse tipologie di programmi; di diversità etnica o demografica di chi dirige il medium, e così via⁶. In particolare, la seconda accezione di *diversity* può sicuramente accrescere le probabilità di un'effettiva diversità di contenuti (e quindi di notizie, temi, opinioni, voci, analisi, ecc.), ma ovviamente non può garantirla.

Il pluralismo esterno trova applicazione nei confronti di tutti i media nella gran parte degli Stati membri; al contrario, gli obblighi di pluralismo interno di norma vengono applicati solo (o in misura di gran lunga prevalente) ai media di servizio pubblico.

La ragione della resistenza ad estendere *tout court* gli obblighi di pluralismo interno anche nei riguardi dei media privati (in tal modo, andando diritti al punto) risiede, nella maggior parte dei casi, in delicati problemi di ordine costituzionale – per giunta, potenzialmente diversi in ogni Stato membro – legati alla tutela della libertà dei media.

Al riguardo, è nota la posizione assunta dalla Corte costituzionale italiana, in base alla quale nei riguardi dei media privati sussistono «maggiori limiti all'estensione del pluralismo [interno] in ragione delle libertà costituzionali assicurate alle imprese dagli artt. 21 e 41 Cost.»⁷, considerato tra l'altro che le emittenti private sono «imprese di tendenza», titolate – come tali – a far emergere una propria «identità politica» attraverso «le proprie analisi e considerazioni di ordine politico»⁸.

Sulla base di queste coordinate costituzionali, sembra perciò che – almeno nell'approccio sin qui seguito dalla Consulta – la possibilità di estendere a tutti i media il rispetto del pluralismo interno sarebbe problematica e che, invece, nell'ottica della Corte, la realizzazione del pluralismo informativo nel suo complesso debba passare attraverso una combinazione di politiche volte a tutelare il pluralismo esterno nel versante privatistico del sistema ed il pluralismo interno nei confronti della concessionaria del servizio pubblico, alla quale vengono affidati compiti di interesse pubblico anche «eccedenti» rispetto al pluralismo strettamente inteso, come quello di operare «per la diffusione della cultura, col fine di “ampliare la partecipazione dei cittadini e concorrere allo sviluppo sociale e culturale del Paese”»⁹ e, quindi, con una finalità di promozione della cultura e della lingua nazionali nonché di inclusione sociale.

Come visto, in linea di massima, il pluralismo esterno e quello interno agiscono, per così dire, di conserva, sicché, per considerare realizzato il pluralismo informativo, occorre perseguire politiche finalizzate a garantire, evidentemente con strumenti diversi, tanto il pluralismo esterno, quanto quello interno.

Ma gli obblighi di pluralismo interno, quando estesi ai media privati, possono entrare in conflitto con il pluralismo esterno e con l'indipendenza dei media, come dimostra, ad esempio, la recente sentenza emessa dalla Corte EDU¹⁰ in relazione ad un

6. Si v. NAPOLI 2011, p. 14.

7. C. cost. n. 420/1994 (par. 14.3 del “considerato in diritto”) che cita le precedenti C. cost. n. 148/1981, C. cost. n. 112/1993, C. cost. n. 826/1988.

8. C. cost. n. 155/2002, par. 2.2 del “considerato in diritto”.

9. C. cost. n. 284/2002, par. 4 del “considerato in diritto”.

10. Corte europea dei diritti dell'uomo [GC], sentenza 5 aprile 2022, ric. n. 24870, caso *NIT s.r.l. c. Repubblica di Moldavia*. Non che in Moldova non vi fosse una “situazione molto difficile” (in piena fase di transizione verso una

caso in cui, con un provvedimento dell'autorità di settore moldava, era stata revocata l'autorizzazione a trasmettere ad una società titolare di un'emittente televisiva (NIT) a causa della ritenuta violazione degli obblighi di pluralismo interno imposti dal codice dell'audiovisivo moldavo vigente all'epoca dei fatti (2012).

NIT avrebbe in particolare tenuto nei suoi notiziari una posizione a favore del Partito comunista moldavo (PCRM), all'epoca l'unico partito di opposizione del Paese, ed inoltre avrebbe negato agli altri partiti di replicare alle accuse loro rivolte dall'emittente.

Chiamata a pronunciarsi su un caso che poneva gli obblighi di pluralismo interno in diretta tensione con la tutela del pluralismo esterno (posto che la chiusura di una "voce", per i suoi notiziari troppo favorevoli all'opposizione, portava inevitabilmente all'impoverimento delle "voci" presenti nel panorama mediatico allora limitato, in quanto ancora analogico), la Corte ha optato per la prima declinazione di pluralismo, nonostante questa scelta finisse con l'impattare direttamente sulla libertà editoriale dell'emittente e sebbene la stessa Corte abbia escluso che le espressioni utilizzate da NIT, per quanto probabilmente «scioccanti, offensive e disturbanti», integrassero incitamento alla violenza, all'odio o alla xenofobia¹¹.

La sentenza ha bensì riconosciuto che gli obblighi di pluralismo interno imposti dalla Moldavia alle emittenti private erano tra i più pervasivi nell'ambito di quelli pur rinvenibili in altri Paesi del Consiglio d'Europa, ma ha ritenuto che essi non si ponessero in contrasto con l'art. 10 CEDU, visto che l'imposizione di siffatti obblighi era volto alla tutela dei «diritti altrui» (dei telespettatori) e rientrava pur sempre nell'«ambito di apprezzamento» del singolo Stato contrattante.

3. Le c.d. nuove sfide al pluralismo informativo

Una serie di avvenimenti e sviluppi, anche tecnologici, hanno posto sotto tensione l'approccio tradizionale alla questione della tutela del pluralismo. Si è trattato di situazioni davvero numerose e multiformi (molte per l'innanzi neppure immaginabili), alcune delle quali possono considerarsi stabili, altre invece circostanziali e non necessariamente destinate a ripetersi periodicamente.

Tra quelle (almeno auspicabilmente) transitorie vanno ricordate la pandemia di COVID – 19 ed il conflitto bellico seguito all'invasione dell'Ucraina da parte della Russia (conflitto in cui l'UE ha preso, assieme agli USA, una posizione nettamente favorevole all'Ucraina, fornendole supporto militare con l'invio di armamenti e training delle truppe), che ha certamente esacerbato l'utilizzo, già in atto, dell'informazione a fini di destabilizzazione delle democrazie occidentali effettuato da potenze straniere (soprattutto Russia e Cina, a quanto pare) e dai loro servizi segreti nell'ambito della c.d. guerra ibrida¹².

Tra le circostanze stabili possono, invece, ricordarsi le posizioni di forza assunte dalle piattaforme digitali di maggiore dimensione non solo dal punto di vista economico ma anche come *gatekeepers* delle informazioni¹³, con i connessi fenomeni di prioritarizzazione algoritmica delle notizie e polarizzazione degli utenti; i tentativi di condizionare le elezioni (si pensi, ad es., alle elezioni USA del 2016); il c.d. *overload* informativo che rende difficile ai cittadini orientarsi su un determinato argomento e di individuare fonti affidabili; ma anche le acquisizioni scientifiche emerse dall'economia comportamentale e dalla sua estensione allo studio del consumo dell'informazione anche attraverso i

moderna democrazia europea: v. par. 202 sentenza), ma il fatto che a pronunciarsi sulla questione sia stata chiamata la Grand Chambre e che questa abbia dichiarato che la soluzione del caso abbia comportato la necessità di «sviluppare la giurisprudenza della Corte sul pluralismo dei media» inducono a ritenere che i principi ivi enunciati non siano da ricollegare solo a circostanze legate alla specificità del caso.

11. *Ivi*, par. 215.

12. Secondo la Treccani online: «strategia militare, caratterizzata da grande flessibilità, che unisce la guerra convenzionale, la guerra irregolare e la guerra fatta di azioni di attacco e sabotaggio cibernetico». Si v. anche FRIDMAN 2018.

13. Si tratta di temi ben noti ed investigati; per ragioni di sintesi sia consentito rinviare a GRANDINETTI 2022.

media tradizionali, con l'evidenziazione dei c.d. *bias cognitivi*¹⁴.

Si tratta di fenomeni che, pur muovendosi su piani diversissimi, hanno inciso profondamente sull'approccio alla tutela della libertà di informazione e del pluralismo e paiono aver creato un contesto favorevole al passaggio da policy volte a creare le migliori condizioni possibili affinché i cittadini possano formarsi un'opinione autonoma e scegliere alla luce delle diverse posizioni ideologiche diffuse sui media ad interventi mirati a valutare "a monte" e direttamente i contenuti diffusi sui vari media.

Talune prese di posizione in tal senso possono comprendersi tenendo conto che in alcune situazioni di estrema emergenza (come pandemie e guerre) le limitazioni alla libertà di espressione e di informazione tendono inevitabilmente ad ampliarsi¹⁵; altre appaiono però sintomo di una tendenza ad un più globale ripensamento rispetto all'approccio tradizionale.

Nella prima categoria, può inquadrarsi, ad esempio, l'adozione da parte del Consiglio Ue¹⁶ di misure atte a proibire la diffusione satellitare dei palinsesti di emittenti controllate, direttamente o indirettamente, dalla Federazione russa (*RT France* e *Sputnik*) e che diffondevano programmi e notizie volti a giustificare e sostenere l'invasione dell'Ucraina da parte della Russia. Adito da *RT France*, il Tribunale UE¹⁷ ha mandato esente da violazioni della libertà di informazione dette misure, mettendo tuttavia più volte in risalto l'eccezionalità della

situazione (conflitto armato alle porte dell'Ue), il finanziamento esclusivo e diretto di *RT France* da parte della Federazione Russa e la mancanza di autonomia editoriale da parte dell'emittente¹⁸. Ciononostante, non sono mancate sia critiche relative alla prevalenza accordata dal Tribunale all'ordine pubblico Ue rispetto alla libertà di informazione, intesa anche come diritto dei cittadini a ricevere notizie; sia perplessità relative alla proporzionalità dell'intervento che ha finito per applicare il rimedio più estremo: quello della sospensione delle trasmissioni dell'emittente¹⁹. Più in generale, le misure adottate sono state percepite in alcuni Paesi come una preoccupante limitazione della libertà di espressione²⁰.

Nella seconda categoria sembra, invece, di dover inserire la già citata sentenza della Corte EDU sul caso NIT.

Sotto tutt'altro profilo, la presa d'atto dell'irrazionalità di molte nostre scelte dovuta ai *bias cognitivi* – che ci spingono a prendere decisioni irrazionali e persino contrarie ai nostri stessi interessi, oltre che ad assumere posizioni decisamente di parte – ha concorso a spostare il focus dal "lato dell'offerta" (cioè, dal lato dei media e del loro pluralismo) a quello della "domanda" (cioè, a quello dei cittadini e delle loro scelte di "consumo" di informazioni e dal reale beneficio che il pluralismo può concretamente produrre a favore di un'opinione pubblica più consapevole). In altri termini, se gli stessi cittadini domandano ai media un'informazione distorta e parziale a causa

14. Cioè, un errore cognitivo sistemico che tendiamo a ripetere senza far tesoro delle eventuali esperienze negative; in argomento, anche per la rilevanza dei *bias* nel contesto dei media, pure tradizionali, si v., ad es., NICITA 2021, *passim*, ma spec. 12 e 86 ss. Più in generale sui *bias* cognitivi e fenomeni collaterali, si v. BONCINELLI-CALVARUSO 2021.

15. È appena il caso di ricordare che, come sottolineato nel *Dialogo* tra Bollinger e Stone, che introduce BOLLINGER-STONE 2019, p. 1 ss., in ben tre casi (Schenck, Frohwerk, Debs) sorti in pieno dibattito sull'entrata in guerra degli USA nella prima guerra mondiale, la Corte Suprema (e persino il giudice Holmes che poco tempo dopo avrebbe redatto la celeberrima *dissenting opinion* a favore del free speech) ritennero non tutelabili anche le più tenui manifestazioni di dissenso contro l'intervento militare americano. Nel senso della ricorrente imposizione di maggiori limiti in situazione di guerra o di emergenza, v. MANETTI 2006, p. 228 e nt. 12.

16. Decisione del Consiglio (PESC) 2022/351 del 1° marzo 2022 ed il coevo Regolamento del Consiglio (UE) 2022/350.

17. Tribunale UE [GC], 27 luglio 2022, caso T-125/22, *RT France c. Consiglio*, sebbene vada sottolineato che (circostanza non trascurabile) l'Ue e i suoi Stati membri non sono mai entrati in guerra contro la Federazione Russa.

18. Nota come queste peculiari circostanze sembrino rappresentare l'effettiva *ratio decidendi* della sentenza MAF-FEO 2022, p. 195 ss.

19. MILLET 2022; in diverso senso si v. CHARVIN 2023.

20. Si v. per l'Irlanda, FLYNN 2023, p. 18 e, per la Svezia, FÄRDIGH 2023, p. 7.

dei loro *bias* e polarizzazioni, l'adozione di misure correttive dal lato dell'offerta (media) potrebbe rivelarsi uno strumento inidoneo a risolvere il problema di un'informazione imparziale e corretta²¹. Si tratta peraltro di un approccio emerso già nei primi anni Duemila (ben prima della comparsa delle piattaforme digitali), quando, ad esempio, la *Federal Communications Commission* americana si è posta il problema se la possibilità, offerta dalla tecnologia già allora disponibile, di attingere a numerose e diverse fonti informative conducesse effettivamente all'acquisizione di un'informazione più pluralistica da parte dei destinatari e, in caso negativo, quali conseguenze avrebbero dovuto trarsene riguardo alla perdurante utilità di regole rigorose a tutela del pluralismo esterno²².

Di qui ad ipotizzare, in un contesto europeo, che un'autorità nazionale di regolazione dotata di competenze tecniche settoriali possa valutare se l'informazione offerta dai media sia "imparziale e corretta" e, dunque, sia di beneficio per i cittadini, il passo può essere breve, potendo persino portare alla riattualizzazione di un'ampia concezione del limite dell'ordine pubblico²³.

Anche a questo proposito sembra naturale investigare se e come tali problemi siano stati affrontati dall'EMFA.

4. Alcune considerazioni generali su EMFA e pluralismo

Prima di passare all'analisi delle singole previsioni più rilevanti ai fini della nozione di pluralismo, sembra opportuno segnalare alcune scelte di fondo

dell'EMFA che hanno probabilmente condizionato *ab origine* l'approccio al tema.

Il primo aspetto è senz'altro quello che, per la prima volta, si è scelto di disciplinare assieme, con previsioni di carattere "trasversale", *tutti* i fornitori di media – cioè, anche la stampa – e non solo i media audiovisivi, già oggetto di numerosi interventi a partire dalla Direttiva TV senza frontiere del 1989 sino alla Direttiva (UE) 2018/1808.

E si è trattato di una scelta tanto più rilevante, in quanto per secolare tradizione normativa molti Stati membri²⁴ e la giurisprudenza delle Corti, non solo europee, hanno sempre tenuto presente che «i media audiovisivi hanno un più immediato e forte impatto rispetto alla stampa», con tutto ciò che ne è conseguito in ordine alla minore interferenza regolatoria sui media scritti, anche (e proprio) a tutela del pluralismo²⁵. Una volta optato nell'EMFA per questo approccio trasversale – distinguendo non tra tipi di media, ma tra doveri dei "fornitori di media" di servizio pubblico²⁶ e no – la previsione, ad esempio, di obblighi di pluralismo interno a carico degli editori della carta stampata sarebbe risultata difficilmente prospettabile.

Quali che siano state le ragioni più profonde di questa scelta²⁷, l'assimilazione tra fornitori di media scritti ed audiovisivi, ai fini dell'individuazione dei loro diritti e doveri, si pone in un rapporto oggettivamente problematico con la risalente differenziazione di disciplina tra i due tipi di media, proprio *sub specie* di tutela del pluralismo.

Questa stessa scelta di fondo può forse spiegare l'equiparazione, per altri versi opinabile²⁸, tra l'assoggettamento del fornitore di servizi media

21. NICITA 2021, p. 168.

22. FEDERAL COMMUNICATIONS COMMISSION 2010. In dottrina, da un punto di vista metodologico, NAPOLI 2011, p. 255 ss.

23. Cui fa, ad es., riferimento NICITA 2021, pp. 198-199, che richiama anche limiti come l'"armonia collettiva" o la "protezione dall'avvelenamento del clima sociale".

24. Sul punto si v., ad es., PACE 1992, p. 177 ss.

25. Per la giurisprudenza della Corte EDU, si v. da *Jersild v. Denmark*, 23 settembre 1994, par. 35, Series A no. 298 sino alla già citata *NIT v. Moldavia* del 2022.

26. Concetto già problematico ove riferito alla stampa, in argomento v. sempre PACE 1992.

27. Sul punto non sembrano dirimenti le giustificazioni contenute nei pertinenti considerando dell'EMFA, come, ad es., la crescente rilevanza transfrontaliera della stampa (cons. 1), la disponibilità di contenuti in diverse lingue, anche grazie ai servizi di traduzione automatica, e la crescente possibilità di combinare, in ambiente digitale, contenuti audiovisivi e non audiovisivi nella stessa offerta (cons. 3).

28. V. BARATA 2022.

alla supervisione di un'autorità nazionale di regolamentazione e l'adesione a un meccanismo di coregolamentazione o di autoregolamentazione relativo alle norme editoriali, ad esempio, al fine della dichiarazione di cui all'art. 18.1 ed al connesso godimento dello speciale trattamento ivi previsto a carico delle piattaforme online di dimensioni molto grandi in caso di sospensione dei servizi di intermediazione basata sulla ritenuta incompatibilità dei contenuti offerti dal fornitore di servizi media ed i termini e condizioni applicati dalla piattaforma (art. 18.4 e cons. 52).

Un altro punto di carattere generale, ma destinato a rilevare particolarmente rispetto al tema in esame, è la scelta del legislatore europeo di lasciare la possibilità agli Stati membri di adottare «norme più dettagliate o più rigorose» in alcuni ambiti²⁹, tra i quali – per ciò che qui più rileva – rientrano i diritti ed i doveri dei fornitori di servizi di media e dei destinatari dei medesimi servizi, nonché le prescrizioni sull'analisi delle concentrazioni e sui provvedimenti che possano comunque incidere sulle attività dei fornitori di servizi di media³⁰.

Al riguardo è, infatti, ben noto come il criterio del massimo standard di protezione di un diritto fondamentale non sia talvolta dirimente, in considerazione del rapporto inevitabilmente “relazionale” sussistente tra i vari diritti fondamentali (*in primis*, nel caso di conflitto tra gli stessi)³¹. Eppure, proprio a tali opinabili valutazioni sembra restare affidata la legittimità di previsioni nazionali che, ad esempio, impongano – a dichiarata garanzia dei diritti dei destinatari dei servizi di media

– stringenti obblighi di pluralismo interno a carico di fornitori di servizi di media non di servizio pubblico (così però restringendone la libertà ed indipendenza editoriale), nonostante l'EMFA sembri – come si dirà più ampiamente *infra* (par. 5) – imporre solo ai media di servizio pubblico l'obbligo di «una copertura mediatica imparziale ed equilibrata» (cons. 27) e l'obbligo di fornire «una pluralità di informazioni e opinioni al loro pubblico» (art. 5.1).

E si tratta di dubbi tutt'altro che teorici, ove solo si consideri che, ad es., l'autorità indipendente francese è intervenuta ripetutamente ed in misura crescente³², in ciò sostenuta da una recente sentenza del Consiglio di Stato, a fronte di violazioni degli obblighi di pluralismo interno derivanti dai contratti di servizio, tra l'altro, per non essere stata garantita una sufficiente diversità di punti di vista nei dibattiti su questioni controverse³³.

Qualora temi come quello appena esaminato dovessero ritenersi inclusi nell'ambito della facoltà degli Stati membri di adottare norme «più dettagliate o più rigorose» (come pure potrebbe sostenersi), dovrebbero essere considerevolmente ridimensionate le ambizioni, enunciate nel preambolo dell'EMFA, di armonizzare la disciplina del settore dei media anche per gli aspetti legati al pluralismo.

Infine, soprattutto nello scenario testé delineato, l'intento “armonizzatore” sotteso all'EMFA dovrebbe essere ricollegato prevalentemente – se non esclusivamente – alle previsioni contenute nella sezione 5 del capo III dell'EMFA (*Prescrizioni*

29. Modifica richiesta nel parere del servizio giuridico del Consiglio per coerenza con la base normativa individuata nell'art. 114 TFUE (Council 2022/0277 (COD)): v. BROGI-BORGES-CARLINI et al. 2023, p. 40, nt. 57.

30. L'art. 1.2 fa testuale riferimento agli ambiti di cui al capo II, al capo III sezione 5 e all'art. 25 (relativo all'allocazione di fondi pubblici per la pubblicità statale e contratti di fornitura di servizi).

31. Lo ricorda assai opportunamente CARTABIA 2017, p. 16; nello stesso senso ed in termini più generali, v. PACE 2003, pp. 46-47, secondo il quale il giudizio «presuppone, a ben guardare, l'attenta considerazione delle *corrispondenti limitazioni* che verrebbero imposte ai titolari dei diritti interdipendenti con il diritto che si intenda “migliorare” (si pensi all'interdipendenza tra le discipline della libertà di riunione in luogo pubblico e della libertà di movimento; della libertà di informazione e del diritto alla riservatezza; del diritto di elettorato passivo e delle libertà economiche; delle azioni “positive” e dell'eguaglianza formale; ecc.)» (enfasi nell'originale).

32. Per una rassegna delle decine di sanzioni (attinenti però anche ad altri aspetti) irrogate alle emittenti “militanti”, come CNEWS del gruppo Bolloré, v. la rassegna svolta da *Le Monde*, 13 marzo 2024, *C8 et CNews: plus de 40 rappels à l'ordre de l'Arcom, dont la moitié depuis trois ans*.

33. Conseil d'État, 13 febbraio 2024, *Reporters sans frontière (RSF) / ARCOM*, par. 16, commentata, ad es., da A. Dimeglio con il significativo titolo *Affaire CNEWS: pluralisme contre liberté?*

per misure e procedure che garantiscano il buon funzionamento del mercato dei media).

In particolare, quanto ad eventuali “malfunzionamenti” attribuibili ad operazioni di concentrazione, entrerebbe in gioco anzitutto l'art. 22 dell'EMFA, che chiarisce come l'impatto previsto dalla concentrazione andrà valutato considerando le conseguenze sulla “diversità dei servizi e dell'offerta dei media sul mercato” (para. 2, lett. a) e che, come ulteriormente precisato dal considerando 64, nell'ambito di tale valutazione «il pluralismo dei media dovrebbe essere inteso come la possibilità di avere accesso a una varietà di servizi di media e contenuti mediatici che trasmettano opinioni, voci e analisi diverse».

In secondo luogo, ai sensi della stessa disposizione, vi sarebbero prima gli “orientamenti” adottati sul punto dalla Commissione (in ciò assistita dal Comitato europeo per i servizi di media: para. 2), e poi, nelle ipotesi di concentrazioni che possano incidere sul funzionamento del mercato interno, l'intervento dello stesso Comitato, chiamato ad esprimere, sul progetto di valutazione dell'autorità del singolo Stato membro, un parere che l'autorità nazionale deve tenere nella massima considerazione, motivando in merito ad eventuali scostamenti dallo stesso parere (para. da 4 a 6).

Per quanto attiene, invece, a “malfunzionamenti” indipendenti da operazioni di concentrazione³⁴, sembrerebbe poter entrare in gioco l'art. 21, che non soltanto prevede che le «misure legislative, normative e amministrative» nazionali incidenti sul pluralismo dei media (o sull'indipendenza editoriale) debbano essere debitamente giustificate e proporzionate, oltre che trasparenti, oggettive e non discriminatorie, con riconoscimento del diritto al ricorso da parte del fornitore individualmente e direttamente interessato (para. da 1 a 3), ma che contempla altresì la possibilità, in caso di misura particolarmente incisiva, che il Comitato europeo per i servizi di media elabori un parere su richiesta della Commissione, d'ufficio nonché su istanza del fornitore interessato (para. da 3 a 5).

Dalla maggiore o minore ampiezza con cui verranno interpretate le previsioni contenute nell'art.

21 dipenderà in gran parte la possibilità dell'Unione di incidere su malfunzionamenti del mercato (tutt'altro che eccezionali nel panorama europeo, ad iniziare dall'Italia), bensì prodotte dalla mancata realizzazione del pluralismo (quantomeno esterno), ma *indipendenti da future operazioni di concentrazione*. Inoltre, posto che le misure di cui all'art. 22 lasciano fuori le situazioni di alta concentrazione preesistenti o causate dalla crescita “spontanea” di un player (ovvero dalla chiusura di un altro)³⁵, una possibilità di intervento su queste situazioni sembra possibile solo attraverso gli strumenti di cui all'art. 21³⁶ (o dall'esercizio di monitoraggio “generale” affidato alla Commissione ai sensi dell'art. 26 dell'EMFA).

È, tuttavia, opportuno ricordare che anche le prescrizioni di cui alla citata sezione 5 rientrano tra quelle in relazione alla quali gli Stati membri conservano la possibilità di adottare norme «più dettagliate o più rigorose», sebbene in questo contesto la valutazione riguardo al maggior dettaglio e rigore potrebbe risultare meno problematica di quanto segnalato in relazione ai diritti e doveri dei fornitori di servizi media.

5. Analisi delle previsioni più rilevanti riguardo al pluralismo

Fatte queste premesse, possono passarsi ad esaminare più analiticamente le previsioni che sembrano maggiormente rilevare ai fini della nozione di pluralismo rintracciabile nell'EMFA.

Non sorprendentemente, tali disposizioni sono contenute soprattutto nel capo II, relativo ai diritti e doveri dei fornitori di servizi di media e (ai diritti) dei destinatari dei medesimi servizi.

Per ragioni di ordine espositivo, è opportuno partire da un dato testuale evidente, e, cioè, che obblighi di pluralismo interno sono *esplicitamente* richiamati solo per i fornitori di media di servizio pubblico. In particolare, l'art. 5.1 impone agli Stati membri di garantire che i media di servizio pubblico «forniscano in modo imparziale una pluralità di informazioni e opinioni al loro pubblico» e, nel preambolo dell'EMFA, la portata di tali obblighi viene ulteriormente dettagliata facendo riferimento

34. Per un analogo inquadramento delle previsioni contenute nella sezione 5 del Capo III, v. COLE-ETTELDORF 2023, pp. 35-36.

35. BROGI-BORGES-CARLINI et al. 2023, p. 75.

36. TAMBINI 2023.

ad obblighi di «un'offerta di contenuti diversificata, comprese informazioni di qualità e una copertura mediatica imparziale ed equilibrata» ed all'obbligo di fornire «informazioni diversificate e promuovere i valori della democrazia, della diversità culturale e della coesione sociale» (cons. 27).

In tal modo, tra l'altro, l'EMFA fornisce – in un atto normativo come un regolamento – un contenuto meno generico al riferimento (contenuto nel Protocollo 29 allegato al TUE ed al TFUE) al contributo essenziale offerto dai media di servizio pubblico «all'esigenza di preservare il pluralismo dei mezzi di comunicazione»³⁷.

Altrettanto rilevante è la previsione relativa all'obbligo degli Stati membri di designare, per i media di servizio pubblico, «una o più autorità o organismi indipendenti o istituire meccanismi liberi da influenze politiche da parte dei governi al fine di monitorare l'applicazione dei paragrafi 1, 2 e 3» (art. 5.4).

A tal fine, è utile contrapporre le previsioni contenute – con riferimento, però, ai fornitori non di servizio pubblico – nell'art. 4, che impone agli Stati membri di rispettare «le effettive libertà editoriali e indipendenza dei fornitori di servizi di media nell'esercizio delle loro attività professionali», escludendo la possibilità che non solo gli Stati, ma anche «gli organismi nazionali di regolamentazione ... interferiscano con le politiche e le decisioni

editoriali dei fornitori di servizi di media ... [o] tent[ino] di influenzarle»³⁸.

In proposito, è opportuno ricordare che, nell'EMFA, viene tracciata – *ad instar* di analoghe previsioni di alcuni Stati membri – una distinzione tra il diritto dei fornitori di servizi di media di definire la *linea editoriale* del medium in una prospettiva di lungo periodo³⁹ (diritto loro riservato nell'esercizio della libertà di impresa e della libertà di espressione⁴⁰) e le *singole decisioni editoriali* da prendere quotidianamente, ad esempio, in merito alla notiziabilità di un evento⁴¹, da riservare invece ai responsabili editoriali e caporedattori e, anzi, da tenere al riparo da influenze da parte dello stesso proprietario del mezzo.

Ma, anche così circoscritto, il diritto del proprietario di imprimere al mezzo la linea editoriale di lungo periodo conferma, in capo al fornitore di servizi di media, un'ampia libertà di esprimere il proprio punto di vista ideologicamente connotato (progressista, conservatore, populista, ecc.), tanto più ove si consideri la riconferma del diritto del fornitore di determinare «la composizione delle ... redazioni» (cons. 35). Del resto, che un fornitore esprima le proprie posizioni, tanto più se «diverse» e «divergenti» da quelle presenti sul mercato, è rappresentato come un aspetto particolarmente rilevante, nello stesso EMFA, per valutare la fattibilità di un'operazione di concentrazione⁴², il che

37. Al contempo, tuttavia, sollevando il delicato problema delle conseguenze derivanti dall'ipotesi che la «missione» affidata dallo Stato membro al fornitore di media di servizio pubblico non contempli il rispetto di obblighi di pluralismo interno: sul punto, v. COLE-ETTELDORF 2023, p. 33.

38. Significativa, al riguardo, la circostanza che non abbia avuto seguito l'emendamento, proposto nel Parere del Comitato delle regioni sulla legge europea per la libertà dei media (2023/C 188/08) del 30 maggio 2023, in base al quale al testo attuale sarebbe stata aggiunta la seguente frase: «..., fatti salvi gli obblighi giuridici – e relative misure di applicazione ed esecuzione – che perseguono obiettivi di interesse generale, in particolare in relazione alla diversità, ai contenuti illegali, alla protezione dei minori nei media o alla definizione di servizio pubblico dei media di servizio pubblico». Al riguardo, COLE-ETTELDORF 2023, p. 21 si interrogano addirittura sulla compatibilità, con l'art. 4.2 dell'EMFA, dell'esercizio delle funzioni assegnate dalla Direttiva (UE) 2010/13 alle autorità nazionali di regolamentazione.

39. Cfr. cons. 34.

40. Cfr. cons. 18.

41. Cfr. la relativa definizione contenuta nell'art. 2.1 n. 7 e citati cons. 18 e 34.

42. Cfr. il cons. 64 in cui viene specificato che «il pluralismo dei media dovrebbe essere inteso come la possibilità di avere accesso a una varietà di servizi di media e contenuti mediatici che trasmettano opinioni, voci e analisi diverse» ed ancora che «[u]n importante criterio da tenere in considerazione è la riduzione di opinioni divergenti all'interno di quel mercato come conseguenza della concentrazione dei media»; ed infine il cons. 68 in cui si legge che le autorità «dovrebbero considerare se altri mezzi di informazione, che forniscono contenuti

implica quantomeno la legittimità dell'attribuibilità di un determinato orientamento al fornitore⁴³.

Si aggiunga che, sotto lo specifico profilo della tutela del *pluralismo* (diversamente da quanto possa probabilmente dirsi del connesso, ma differente, problema dell'indipendenza e dell'integrità dei media⁴⁴), non dovrebbe fare troppa differenza che i destinatari dei media ricevano informazioni condizionate da un certo orientamento per scelta del fornitore o per le scelte dei responsabili editoriali e dei caporedattori o per entrambe.

Si viene così a uno dei punti forse più problematici dell'intera questione, cioè ai diritti dei destinatari dei servizi di media. L'art. 3 dispone che gli Stati membri «rispettano il diritto dei destinatari dei servizi di media di avere accesso a una pluralità di contenuti mediatici editorialmente indipendenti e garantiscono l'esistenza di condizioni quadro conformi al presente regolamento per salvaguardare tale diritto, a beneficio di un dibattito libero e democratico».

Al di là della qualificazione in termini di «diritto» della situazione di cui sono titolari i destinatari dei media, la disposizione è in realtà piuttosto vaga e timida nell'individuazione dei contorni di tale diritto⁴⁵.

Dal punto di vista strutturale, la norma è significativamente cambiata nel corso del procedimento di approvazione: dalla versione della Commissione, in cui si affermava che i destinatari «hanno il diritto di ricevere una pluralità di notizie e contenuti ...», si è passati alla versione definitiva in cui significativamente, dal riconoscimento

di un diritto di derivazione eurounionale, si passa ad un obbligo imposto agli Stati membri di rispettare un siffatto diritto. Ed ancora più eloquente è che una delle motivazioni fornite per la modificazione della formulazione sia stata che tale diritto, sebbene «giuridicamente riconosciuto ... deve essere ulteriormente definito, nonché ponderato rispetto ad altri interessi giuridici»⁴⁶, con ogni plausibilità quelli dei fornitori di servizi di media⁴⁷.

Inoltre, il considerando 14, nel mentre ribadisce che «i destinatari dei servizi di media dovrebbero poter accedere a servizi di media di qualità ...», specifica – in fine – che «[d]al diritto a una pluralità di contenuti dei media non deriva alcun *obbligo* corrispondente per i fornitori di servizi di media di rispettare norme che non siano esplicitamente stabilite *per legge*». Considerato che l'EMFA è, per definizione, la «legge europea per la libertà dei media», questa specificazione lascia intendere che l'art. 3 non possa essere considerato (anche tenendo conto di una certa sua ambiguità, di cui si dirà subito appresso) la fonte di obblighi a carico dei fornitori di media. Ci troveremmo, insomma, di fronte a diritti (in capo ai destinatari) senza corrispondenti obblighi (in capo ai fornitori di servizi di media)⁴⁸.

Ove poi il riferimento alla «legge» fosse alla normativa *nazionale*, le ambizioni armonizzatrici dell'EMFA dovrebbero essere ulteriormente ridimensionate, rispetto a quanto già osservato nel precedente par. 4 ed il regolamento in commento, nonostante tale sua natura⁴⁹, si presenterebbe

diversi e alternativi, continuerebbero a coesistere nel mercato o nei mercati interessati se viene attuata la concentrazione dei media in questione».

43. Per un'argomentazione in parte analoga v. BROGI-BORGES-CARLINI et al. 2023, p. 68.

44. Aspetti che nel presente lavoro non vengono affrontati se non per quanto strettamente collegato alla tutela del pluralismo.

45. Per una più ampia discussione sul punto nella stessa direzione del testo v. COLE-ETTELDORF 2023, pp. 25-26.

46. Si v. la motivazione del relativo emendamento contenuto nel Parere del Comitato delle regioni sulla legge europea per la libertà dei media (2023/C 188/08).

47. Di contro, la formulazione dell'art. 4, relativa ai diritti dei fornitori, recita ancora che i «fornitori di servizi di media hanno il diritto ...», rientrando ovviamente la fornitura di servizi media a pieno titolo nel novero delle tradizionali libertà fondamentali Ue. Peraltro, per BARATA 2024, l'EMFA non riconoscerebbe diritti direttamente azionabili neppure ai fornitori di servizi di media.

48. *Per incidens*, in linea con l'impostazione, riguardo al «diritto all'informazione», espressa da PACE 2007.

49. COLE-ETTELDORF 2023, p. 26, con specifico riferimento al «diritto» dei destinatari, notano come una previsione non avente concrete conseguenze poco si addica ad un regolamento.

ancora di più come un testo quadro che, per molti aspetti attuativi, rinvierebbe alle legislazioni degli Stati membri, con un andamento circolare che certo non giova all'effettività delle disposizioni eurounionali⁵⁰.

Anche dal punto di vista contenutistico la formulazione dell'art. 3 risulta tutt'altro che chiara: in particolare, rimane dubbio se la pluralità dei contenuti mediatici, per il legislatore europeo, dovrebbe essere realizzata nell'ambito del singolo mezzo (*id est*, pluralismo interno) o nell'ambito della complessiva offerta (pluralismo esterno).

Come si esporrà più ampiamente *infra*, in sede di considerazioni conclusive (par. 7), il quadro che ci restituisce l'analisi dettagliata delle singole disposizioni dell'EMFA sembra tutt'altro che univoco sull'effettiva portata di tali previsioni.

6. L'EMFA e le risposte ad alcune delle c.d. nuove sfide al pluralismo

Tra quelle che vengono solitamente definite le nuove sfide al pluralismo (par. 3) rientrano certamente la lotta alla disinformazione ed i meccanismi di moderazione e/o prioritarizzazione di determinati contenuti applicati, sulla base di scelte eminentemente commerciali, da piattaforme online, fabbricanti di dispositivi e fornitori di interfacce.

Il legislatore europeo si è dimostrato sul punto ben consapevole del carattere necessariamenteolitico della risposta a tali nuove sfide, facendo "rete" con i regolamenti già adottati in tema di equità e trasparenza per gli utenti commerciali delle piattaforme online (n. 2019/1150) ed in tema di mercato unico dei servizi digitali (n. 2022/2065), nonché, ove necessario, rafforzando la posizione dei fornitori di servizi di media nei rapporti con le piattaforme online di dimensioni molto grandi.

Le risposte dell'EMFA a questi due temi (disinformazione e prioritarizzazione) possono rintracciarsi, rispettivamente, nella garanzia dell'indipendenza ed integrità editoriale dei fornitori di servizi di media, da un lato, e, dall'altro lato, nell'introduzione di regole di personalizzazione dell'offerta e nella conferma della c.d. *prominence* (debito rilievo) dei servizi di media di interesse generale ai sensi dell'art. 7-*bis* della Direttiva (UE)

2010/13, come modificata dalla Direttiva (UE) 2018/1808.

Quanto al primo punto (indipendenza ed integrità editoriale), le previsioni dell'EMFA individuano le entità rispetto alle quali dovrebbe operare il requisito in parola, vale a dire non solo nei riguardi degli Stati membri, di partiti politici, di paesi terzi ed entità controllate o finanziate da questi ultimi (art. 18.2.c), ma anche degli stessi fornitori di servizi di media nel caso di fornitura di notizie e contenuti di attualità (art. 6.3). In particolare, i fornitori dovrebbero garantire che direttori editoriali e caporedattori possano adottare liberamente le decisioni editoriali (pur nell'ambito della linea editoriale decisa dallo stesso fornitore: v. *supra* par. 5) e segnalino eventuali conflitti di interessi tra notizie e fornitore.

Nella Raccomandazione (UE) 2022/1634 in tema di garanzie interne di indipendenza editoriale (adottata coevamente alla proposta di legge poi divenuta l'EMFA) la Commissione ha offerto un ampio catalogo di possibili strumenti per garantire tale requisito, dai quali si evince tra l'altro l'auspicabilità di una separazione tra attività editoriali e commerciali, in modo da evitare contaminazioni a scapito dell'integrità dell'informazione.

Nella prospettiva dell'EMFA l'accesso dei destinatari a contenuti prodotti da giornalisti in modo indipendente ed in linea con gli standard riconosciuti rappresenta la migliore garanzia della fornitura di notizie affidabili e un antidoto alla disinformazione e alla manipolazione dell'informazione, nonché alle ingerenze di attori stranieri (cons. 14).

L'adozione di tali misure (obbligatorie per i soli fornitori di notizie e contenuti di attualità: art. 6.3) viene poi incentivata, nei confronti di tutti i fornitori di servizi di media, attraverso la previsione di un trattamento "privilegiato" nei casi di sospensione dei servizi di intermediazione, da parte delle piattaforme online di dimensione molto grande, a carico di fornitori di servizi di media che abbiano dichiarato di essere soggetti alla supervisione di un'autorità nazionale di regolamentazione o di aver aderito a un meccanismo di coregolamentazione o di autoregolamentazione che disciplina le norme editoriali (art. 18.1). Si tratta peraltro di una

50. Per giunta, a seguire il testo dell'art. 3, gli Stati membri potrebbero limitarsi anch'essi a garantire l'esistenza di "condizioni quadro".

garanzia che va ad incidere anche sulle politiche di moderazione dei contenuti effettuate dalle piattaforme online di dimensione molto grande.

Passando, allora, al secondo tema (prioritarizzazione di determinati contenuti), l'EMFA per un verso conferma il già richiamato meccanismo della *prominence* dei servizi di media audiovisivi di "interesse generale" e, per altro verso, riconosce agli utenti un diritto alla personalizzazione dei servizi di media accessibili attraverso qualsiasi dispositivo o interfaccia utente.

Quanto alla conferma della *prominence*, sembra opportuno però richiamare, ancora una volta, il rischio che, attraverso questo meccanismo, si finisca – con una vera e propria eterogenesi dei fini – col rafforzare la posizione dei fornitori di media già dominanti in singoli Paesi, così come rischia di avvenire nel nostro Paese a causa delle modalità di attuazione di tale rimedio in sede nazionale⁵¹.

Riguardo alla personalizzazione di dispositivi e interfacce utente, l'EMFA impone ai fabbricanti e importatori di includere una funzionalità che consenta agli utenti di modificare liberamente e facilmente le configurazioni che controllano e gestiscono l'accesso ai servizi di media offerti ed il loro utilizzo (art. 20.2), all'evidente fine di garantire ai destinatari dei servizi di poter scegliere realmente i contenuti che desiderano guardare ed ascoltare, al riparo da condizionamenti derivanti dalle impostazioni predefinite dai produttori di *device*, spesso sulla base di accordi commerciali con i fornitori di determinati servizi di media (cons. 57).

7. Considerazioni conclusive

La disamina sin qui svolta sembra lasciare l'interprete dinanzi ad almeno due diverse opzioni ermeneutiche.

In base ad una prima possibile lettura (certamente più condivisa e, forse, più realistica), una serie di caratteristiche dell'EMFA dovrebbero indurre a considerarlo, *a fortiori* per l'individuazione della nozione del pluralismo, più simile ad una direttiva di armonizzazione (minima) che ad un regolamento⁵². Invero, la formulazione di alcune disposizioni dell'EMFA è tutt'altro che precisa, individuando spesso "principi" che resterebbero poi affidati alla concreta applicazione degli Stati membri i quali inevitabilmente procederebbero poi a declinarli conformemente alle loro tradizioni nella regolamentazione dei media⁵³.

In quest'ottica, sarebbe inevitabile che l'EMFA abbia in concreto un basso impatto sugli ordinamenti giuridici degli Stati membri più avanzati⁵⁴ e, al più, si ponga come un set di principi minimi per i paesi meno garantisti, fungendo al contempo da argine a (sempre possibili) arretramenti di disciplina negli altri Stati membri.

Le ampie concessioni, contenute nell'EMFA, a normative nazionali «più dettagliate o più rigorose», il fatto che il regolamento non attribuisca diritti individualmente azionabili, il rinvio agli Stati membri ed alle loro normative al fine di assicurare il concreto "rispetto" di diritti ed obblighi solo "evocati" nell'EMFA (v. *supra* par. 5) confermerebbero la *reale* portata dell'EMFA.

La naturale conseguenza sarebbe che l'efficacia dell'intervento di armonizzazione – realizzato per giunta per mezzo di un regolamento – ne risulterebbe significativamente indebolita, con la quasi certezza che gli ostacoli al mercato interno non vengano effettivamente superati, anche a seguito dell'EMFA⁵⁵.

Non sembra tuttavia da escludere un'interpretazione, per così dire, "meno riduttiva" della portata dell'intervento, quantomeno "di default": cioè, in

51. Sul punto sia consentito rinviare a GRANDINETTI 2024, p. 21 ss. (spec. 50 ss.). Il paradossale risultato di rafforzare le dinamiche oligopolistiche, anziché la pluralità dei media, è richiamato – sia pure con riferimento alle norme italiane sul SIC ed alla sentenza della Corte di giustizia, 3 settembre 2020, C-719/18 – anche nel preambolo dell'EMFA: v. cons. 63.

52. COLE-ETTELDORF 2023, p. 20.

53. BROGI-BORGES-CARLINI et al. 2023, p. 39.

54. *Ibidem*.

55. Come notato da BROGI-BORGES-CARLINI et al. 2023, p. 67: «On one hand, this diversity respects the national competences and the specificities of each media system, reflecting the different historical, economic and social diverse backgrounds. On the other hand, it could hamper effectiveness of the same rules, in a market that is

manca di normative nazionali «più dettagliate o più rigorose»⁵⁶.

In primo luogo, anche a voler convenire sulla portata minima dell'armonizzazione realizzata con l'EMFA, resterebbe pur sempre difficilmente contestabile che il legislatore eurounioniale si è espresso riguardo a *quali* soggetti vadano applicati *alcune* delle classiche declinazioni del pluralismo.

L'obbligo imposto agli Stati membri di assicurare che i media di servizio pubblico rispettino obblighi di *pluralismo interno* («forniscano in modo imparziale una pluralità di informazioni e opinioni al loro pubblico») rappresenta già una prima opzione in merito alla nozione di pluralismo (ed alle sue declinazioni) tutt'altro che di secondaria importanza⁵⁷.

Per contro, le previsioni relative ai fornitori di media non di servizio pubblico sembrano indicare una netta preferenza per il *pluralismo esterno*; si pensi, ad esempio, all'esclusione dell'intervento non solo degli Stati membri, ma anche delle autorità nazionali di regolamentazione, riguardo alle politiche e decisioni editoriali, rispettivamente, di fornitori di servizi media e di responsabili e caporedattori; al riconoscimento del diritto di imprimere una linea editoriale di lungo periodo; all'esclusione del sorgere di obblighi, in capo ai fornitori di

servizi di media, come *pendant* del «diritto» dei destinatari dei medesimi servizi (v. *supra* par. 5).

Non può, del resto negarsi che – come evidenziato in dottrina⁵⁸ – obblighi di informazione «imparziale, oggettiva, bilanciata» possono, *nelle mani sbagliate*, portare a risultati opposti a quelli perseguiti con la disciplina a tutela del pluralismo⁵⁹.

Entra così in campo un altro tema di particolare importanza, vale a dire la garanzia dell'indipendenza politica delle autorità nazionali di regolamentazione⁶⁰.

Può risultare illusorio il tentativo di «neutralizzare» l'ingerenza statale sull'autonomia editoriale dei media attraverso l'attribuzione del compito di far rispettare il pluralismo interno ad un'autorità nazionale di regolamentazione (ANR)⁶¹.

Come emerge dalle analisi a livello Ue, le procedure di nomina delle ANR rimangono uno dei maggiori rischi proprio con riferimento alla loro indipendenza effettiva. Ad esempio, per quanto attiene al nostro Paese, non tranquillizza il fatto che l'AGCOM ottenga, nelle stesse analisi, un rating di «rischio basso», nonostante venga riscontrato un costante e preoccupante fenomeno di «porte girevoli» tra ruoli politici e nomina dei componenti dell'autorità⁶².

La possibilità che, nell'esercizio di poteri molto intrusivi nell'autonomia editoriale del fornitore⁶³,

more and more interconnected and globalised; and pave the way to the risk, on the State's side, of an use of the rules for other objectives not necessarily related to media pluralism, rising barriers to the circulation in the internal market; and, on the market's side, of a «regime shopping» by the media companies, in search of the most favourable rules for the mergers».

56. Naturalmente, ove si vogliano includere gli aspetti legati al pluralismo tra gli «ambiti» in cui gli Stati membri possano adottare tali misure, ai sensi dell'art. 1.3 dell'EMFA: ma su ciò v. nel testo par. 4.

57. A meno di voler interpretare l'art. 5.1 come espressione di una mera «aspettativa»: in tal senso, v. COLE–ETTELDORF 2023, p. 33, tuttavia con argomentazioni che appaiono in contrasto con la formulazione vincolante della stessa previsione.

58. TAMBINI 2022, p. 311.

59. HOLTZ-BACHA 2024, pp. 38-39, ricordano l'utilizzo strumentale fatto in Ungheria dell'obbligo di «balanced reporting».

60. Come ricordano BROGI–BORGES–CARLINI et al. 2023, p. 70. «it is of the utmost importance reinforcing and guaranteeing their independence [of NRA] from the political power. This would reflect in the independence and well-functioning of the Board. The role of the Commission in issuing the guidelines for the assessment and should be carefully evaluated, as a clearer separation of the different institutional levels would strengthen the independence of the procedure».

61. EUROPEAN UNION 2022, pp. 3 e 44 ss.

62. EUROPEAN UNION 2023, pp. 16-17.

63. Per avere un esempio dell'intrusività che può assumere un siffatto sindacato, si v. le contestazioni formulate dall'AGCOM nella delibera n. 69/20/CONS del 14 febbraio 2020, 21 ss.

possa entrare una “contrattazione politica” (a causa della mancanza di garanzie di imparzialità nelle procedure di nomina dei suoi componenti) è un rischio inaccettabile⁶⁴.

Sotto altro profilo, prima di derubricare la portata dell'EMFA, non dovrebbero essere tralasciate le potenzialità insite nelle previsioni contenute nella sezione 5 del Capo III, contenente le prescrizioni per misure e procedure che garantiscano il buon funzionamento del mercato dei media.

Come si è notato più sopra (par. 4), le misure ivi disciplinate potrebbero rappresentare gli strumenti più incisivi, tanto più che, ai sensi dell'art. 22.3, la Commissione sarà chiamata ad adottare suoi orientamenti in ordine, *inter alia*, all'impatto delle concentrazioni sul pluralismo dei media (compresi i suoi effetti sulla formazione dell'opinione pubblica e sulla diversità dei servizi e dell'offerta dei media sul mercato). Un'occasione, secondo alcuni, grazie alla quale possa essere trasferita a livello Ue il compito di definire cose debba intendersi per “pluralismo dei media”⁶⁵.

Da ultimo, con riferimento ai temi della disinformazione e della prioritarizzazione, le risposte dell'EMFA sembrano equilibrate e realistiche.

L'aver puntato, riguardo alla disinformazione, sull'attività professionale dei giornalisti (sottoposti, almeno in teoria, ad obblighi deontologici) e, quindi, sulla garanzia della loro indipendenza e integrità appare come una scelta quasi “obbligata” ed

è comunque più in diretto rapporto con la sfida da affrontare (certamente più in linea rispetto al tema del pluralismo dei media, in cui l'insistenza sull'indipendenza dei giornalisti appare frutto di una visione forse troppo ottimistica del reale effetto positivo che i giornalisti possono svolgere al riguardo).

Infine, l'intervento relativo al c.d. “lato della domanda” dell'informazione (quello delle scelte dei destinatari dell'informazione) segue la linea del c.d. *nudging* (spinta gentile) nei confronti dei destinatari dell'informazione. Di più sembrava davvero difficile fare, senza invadere aree delicatissime della sfera di autonomia nelle scelte informative riservata a ciascun individuo in forza di diritti fondamentali di libertà individuale.

Certo, ove si parta dalla opposta premessa (di tipo paternalistico) che, a causa dei *bias* cognitivi e della polarizzazione (par. 3), gli stessi cittadini domandino ai media un'informazione distorta e parziale, il riconoscimento di un diritto, in favore del destinatario delle notizie, di poter prioritarizzare i contenuti secondo le proprie scelte e preferenze (par. 6) potrebbe essere considerato ineffettuale a correggere le distorsioni “dal lato della domanda”.

E, tuttavia, quello di mettere al riparo i destinatari da condizionamenti derivanti dalle impostazioni predefinite dai produttori di *device*, spesso sulla base di accordi commerciali con i fornitori di determinati servizi di media, appare comunque un obiettivo da perseguire.

Riferimenti bibliografici

- J. BARATA (2024), *Will the EMFA Improve Freedom of Expression, Media Pluralism, and Media Independence in Europe?*, in “MediaLaws”, 2024
- J. BARATA (2022), *Protecting Media Content on Social Media Platforms: The European Media Freedom Act's Biased Approach*, in “Verfassungsblog”, November 2022
- L.C. BOLLINGER, G.R. STONE (eds.) (2019), *The Free Speech Century*, Oxford University Press, 2019
- E. BONCINELLI, A. CALVARUSO (2021), *Che cosa abbiamo nella testa?*, il Saggiatore, 2021
- E. BROGI, D. BORGES, R. CARLINI et al. (2023), *The European Media Freedom Act: media freedom, freedom of expression and pluralism*, Technical Report, European Parliament, 2023
- M. CARTABIA (2017), *Convergenze e divergenze nell'interpretazione delle clausole finali della Carta dei diritti fondamentali dell'Unione europea*, in “Rivista AIC”, 2017, n. 3

64. Per una critica basata su argomenti del tutto sovrapponibili, si v. la *dissenting opinion* redatta dai giudici Lemmens, Jelić e Pavli, nel caso *NIT s.r.l. c. Repubblica di Moldavia*.

65. COLE-ETTELDORF 2023, p. 36.

- B. CHARVIN (2023), *Good Bye, Putin! La guerre informationnelle a-t-elle sonné le glas du pluralisme? Réflexion sur l'arrêt du Tribunal de l'Union européenne relatif à la suspension de RT France (aff. n° T-125/22, 27 juillet 2022)*, in "La Revue des Droits de l'Homme", 2023
- M.D. COLE, C. ETTELDORF (2023), *Research for CULT Committee – European Media Freedom Act - Background Analysis*, European Parliament, Policy Department for Structural and Cohesion Policies, Brussels, 2023
- EUROPEAN UNION (2023), *Country Report Italy*, Publications Office of the European Union, 2023
- EUROPEAN UNION (2022), *Study on media plurality and diversity online*, Publications Office of the European Union, 2022
- M.A. FÄRDIGH (2023), *Monitoring media pluralism in the digital era: application of the Media Pluralism Monitor in the European Union, Albania, Montenegro, the Republic of North Macedonia, Serbia and Turkey in the year 2022*, Country report: Sweden, European University Institute, 2023
- FEDERAL COMMUNICATIONS COMMISSION (2010), *2010 Quadrennial Regulatory Review – Review of the Commission's Broadcast Ownership Rules and Other Rules Adopted Pursuant to Section 202 of the Telecommunications Act of 1996*, 2010
- R. FLYNN (2023), *Monitoring media pluralism in the digital era: application of the Media Pluralism Monitor in the European Union, Albania, Montenegro, the Republic of North Macedonia, Serbia and Turkey in the year 2022*, Country report: Ireland, European University Institute, 2023
- O. FRIDMAN (2018), *Russian Hybrid Warfare, Resurgence and Policization*, Oxford University Press, 2018
- O. GRANDINETTI (2024), *La tutela del pluralismo nell'era della convergenza digitale*, in R. Mastroianni, O. Pollicino, M. Bassini (a cura di), "Il T.U. dei servizi di media audiovisivi", Giuffrè, 2024
- O. GRANDINETTI (2022), *Le piattaforme digitali come "poteri privati" e la censura online*, in "Rivista italiana di informatica e diritto", 2022, n. 1
- C. HOLTZ-BACHA (2024), *Freedom of the media, pluralism and transparency. European media policy on new paths?*, in "European Journal of Communication", vol. 39, 2024, n. 1
- A. MAFFEO (2022), *La sottile linea di confine tra libertà di informazione e propaganda di guerra: il caso RT France*, in R. Mastroianni, F. Ferraro (a cura di), "Libertà di informazione e diritto dell'Unione europea", Editoriale Scientifica, 2022
- M. MANETTI (2006), *Limiti oggettivi. L'ordine pubblico nelle democrazie pluralistiche*, in A. Pace, M. Manetti, "La libertà di manifestazione del proprio pensiero", Zanichelli, 2006
- R. MASTROIANNI (2022), *Libertà e pluralismo dei media: un valore europeo ancora da scoprire?*, in R. Mastroianni, F. Ferraro (a cura di), "Libertà di informazione e diritto dell'Unione europea. Le nuove sfide a tutela della democrazia e del pluralismo", Editoriale Scientifica, 2022
- R. MASTROIANNI, F. FERRARO (a cura di) (2022), *Libertà di informazione e diritto dell'Unione europea*, Editoriale Scientifica, 2022
- F.X. MILLET (2022), *Suspension de RT France, le dilemme entre mesure d'exception et respect de la liberté d'expression*, in "FigaroVox", 23 août 2022
- A. NICITA (2021), *Il mercato delle verità*, il Mulino, 2021
- P.M. NAPOLI (2011), *Exposure Diversity Reconsidered*, in "Journal of Information Policy", vol. 1, 2011
- L. NJAKAS et al. (2018), *Internal Media Plurality in Audiovisual Media Services in the EU: Rules & Practices*, 2018
- OFCOM (2015), *Measurement framework for media neutrality: Ofcom's advice to the Secretary of State for Culture, Media and Sport*, 5 November 2015

- A. PACE (2007), *Libertà di informare e diritto ad essere informati: due prospettive a confronto nell'interpretazione e nelle prime applicazioni dell'art. 7, primo comma, del T.U. della radiotelevisione*, in *Diritto pubblico*, 2007, n. 2
- A. PACE (2003), *Problematica delle libertà costituzionali. Parte generale: Introduzione allo studio dei diritti costituzionali*, Cedam, 2003
- A. PACE (1992), *Comunicazioni di massa*, in "Enciclopedia delle scienze sociali", Treccani, 1992
- D. TAMBINI (2023), [*The EU is taking practical measures to protect media freedom. Now we need theory*](#), Centre for Media Pluralism and Media Freedom, 2023
- D. TAMBINI (2022), *Reconceptualizing Media Freedom*, in M. Moore, D. Tambini (eds.), "Regulating Big Tech: Policy Responses to Digital Dominance", Oxford University Press, 2022



ANTONIO MANGANELLI – MARIA LUCE MARINIELLO

La valutazione delle concentrazioni per la tutela del pluralismo informativo

Il nuovo regolamento EMFA prevede per la prima volta una disciplina armonizzata per il controllo delle concentrazioni nei mercati dei media. Tale armonizzazione è sia sostanziale sia essenzialmente procedurale, andando a definire nuovi assetti organizzativi e funzionali delle autorità indipendenti preposte ed un nuovo sistema di governance istituzionale. Sotto un profilo sostanziale, la *market plurality* è garantita dalla stretta connessione fra gli obiettivi di “pluralità dei media”, da un lato, e di “indipendenza editoriale”, dall’altro lato, che sembra andare a sfumare la netta distinzione rinvenibile in alcuni ordinamenti nazionali fra i concetti di pluralismo esterno ed interno, anche in relazione all’ambiente media ed informativo digitale. In particolare riferimento all’ordinamento italiano, la disciplina definita dal Testo Unico dei Servizi Media Audiovisivi (TUSMA) sembra, da un lato, essere sostanzialmente allineata con il nuovo impianto normativo europeo e, dall’altro, fornire già alcuni esempi attuativi coerenti con le disposizioni che richiedono la definizione di nuovi indicatori e metodologie ai fini del *market plurality test*.

*Concentrazioni dei media – Concorrenza e pluralismo – Valutazione di impatto sul pluralismo
Assetto istituzionale – Piattaforme digitali*

Media concentration and plurality test

The European Media Freedom Act (EMFA) envisages for the first time a harmonised discipline for the control of concentrations in the media markets. This harmonisation is both substantial and essentially procedural, defining new organisational structures for the authorities in charge and a new system of institutional governance. From a substantive point of view, market plurality is guaranteed by the necessary interconnection between the objectives of “media plurality”, on the one hand, and “editorial independence”, on the other hand, which seems to blur the existing clear distinction, in some national legal frameworks, between the concepts of external and internal pluralism, especially in relation to the digital media and information environment. Finally, the Italian Code of Audio-Visual Media Services (TUSMA) seems to be substantially aligned with EMFA’s provisions, and the guidelines already adopted by AGCOM may probably represent a national good practice and, possibly, a reference model for the future adoption of the Commission’s orientations for the purposes of the market plurality test required by EMFA.

*Media concentration – Competition and pluralism – Media plurality test – Institutional governance
Digital platforms*

A. Manganelli è professore di Diritto e politiche della concorrenza all’Università degli Studi di Siena

M.L. Mariniello è funzionaria di ruolo esperta di area giuridica - Servizio per l’attività internazionale e i rapporti con l’Ue presso l’Autorità per le garanzie nelle comunicazioni (AGCOM)

Sebbene il contributo sia frutto di riflessioni congiunte, i paragrafi 1 e 3 sono attribuibili a M.L. Mariniello ed i paragrafi 2 e 4 ad A. Manganelli. Le valutazioni, le opinioni e i commenti sono formulati in questo scritto a titolo meramente personale e non impegnano in alcun modo l’Autorità per le garanzie nelle comunicazioni

Questo contributo fa parte della sezione monografica *EMFA under the spotlight: towards a common regulatory framework to foster media plurality?* a cura di Elda Brogi

SOMMARIO: 1. La valutazione delle concentrazioni dei media nel Regolamento EMFA. – 2. Il “pluralismo” informativo e i suoi indicatori nell’attività di controllo delle concentrazioni. – 3. La valutazione di impatto sul pluralismo come nuova funzione regolatoria nel sistema di governance dei media. – 4. L’implementazione a livello nazionale: la disciplina italiana del TUSMA e la sua recente evoluzione.

1. La valutazione delle concentrazioni dei media nel Regolamento EMFA

Il livello di concentrazione della proprietà nel settore dei media è correlato con il potere economico e l’indipendenza editoriale nel sistema dell’informazione¹. A differenza degli altri settori industriali, il potere nel settore dei media non è solamente un potere di mercato, che può sfociare in una dominanza² e, quindi, nella capacità di influenzare unilateralmente le dinamiche di prezzo e altre condizioni di fornitura di beni o servizi. Nel settore dei media, questo potere si riferisce, anche e primariamente, alla capacità di influenzare l’opinione pubblica e, quindi, al potenziale impatto negativo su diritti fondamentali degli individui ed anche sul funzionamento stesso del processo democratico.

Nel sistema dell’informazione e dei media, la Corte costituzionale italiana ha infatti tradizionalmente ravvisato un collegamento funzionale fra il profilo passivo della libertà di espressione del pensiero, il diritto all’informazione, ed il pluralismo informativo, ove «il pluralismo si manifesta nella concreta possibilità di scelta, per tutti i cittadini, tra una molteplicità di fonti informative»³. Nella sua nota giurisprudenza, la Corte distingue i concetti

di pluralismo interno (o nella fonte) e pluralismo esterno (o delle fonti) riferendoli, rispettivamente, alla funzione specifica esercitata dall’emittente pubblica ed ai contesti in cui una pluralità di media (di proprietà pubblica e/o privata) possano operare in condizioni di concorrenza nel mercato, al fine di «favorire l’accesso nel sistema radiotelevisivo del massimo numero possibile di voci diverse»⁴.

Ciò nonostante, la tendenza alla concentrazione della proprietà è un fenomeno strutturale nel settore dei media, in ragione della “storica” presenza di barriere all’entrata, sia di carattere tecnico, ad esempio la scarsità di risorse frequenziali (per il *broadcasting*), sia di carattere economico, quali gli alti costi fissi per lo sviluppo delle infrastrutture e (in alcuni contesti) le economie di rete (i.e., economie di rete dirette, ad esempio nella diffusione di contenuti su reti di telecomunicazione, ed economie di rete indirette per quanto concerne la disponibilità di risorse pubblicitarie⁵). Tale tendenza è ulteriormente aumentata nell’ambiente digitale, prevalentemente in ragione dell’evoluzione tecnologica dei mercati dei media e della concorrenza, più o meno diretta, che le piattaforme digitali (sia di streaming sia di condivisione video) e le fonti algoritmiche di contenuti multimediali ed

1. Si tratta di due concetti chiave richiamati, con particolare riguardo all’affermazione delle piattaforme online globali, già nelle premesse dello *European Media Freedom Act* (si v. in particolare il considerando 4), oggetto di questo contributo.

2. Ossia la capacità di comportarsi in misura apprezzabilmente indipendente dai concorrenti e dai consumatori. Sentenza CGUE 14 febbraio 1978, *United Brands Company e United Brands Continentaal BV*, C-27/76, 65.

3. Corte Cost., sentenza n. 826 del 1988.

4. Corte Cost., sentenza n. 112 del 1993.

5. Per una definizione e descrizione delle differenze si veda CAMBINI–MANGANELLI –NICITA 2024.

informativi esercitano, in modo diverso, sui vari versanti di tali mercati.

Al fine di perseguire e tutelare il valore del pluralismo “esterno” – inteso come offerta di una pluralità di voci da parte del mercato – in diversi Stati membri dell’Unione europea, e in particolare nell’ordinamento italiano, sono state definite discipline speciali anti-concentrative per il settore dei media, a complemento della prospettiva economica del diritto della concorrenza. Tuttavia, questa distinzione e specificazione non sempre è stata considerata necessaria, anche in ragione del fatto che il Regolamento concentrazioni 139/2004/CE (art. 21.4) lascia agli Stati la prerogativa di scrutinare le concentrazioni che sollevano legittime preoccupazioni di interesse pubblico, consentendone il divieto in base a criteri più ampi e diversi da quelli della concorrenza (tra cui il pluralismo nei mezzi di comunicazione)⁶.

In ogni caso, diversamente da altri ambiti di disciplina dei media audiovisivi, che hanno trovato un crescente coordinamento ed armonizzazione per mezzo delle direttive su servizi media audiovisivi (SMAV)⁷, il principio del pluralismo dei media nella sua accezione di garanzia della *market plurality* – intesa come pluralità e diversità non solo di fonti informative e mezzi di comunicazione

ma anche dei soggetti proprietari⁸ – ha avuto uno sviluppo normativo autonomo e differenziato nei diversi ordinamenti nazionali⁹. Questo è vero soprattutto per quanto riguarda il sistema di regolazione pubblica a tutela della trasparenza degli assetti proprietari e della concorrenza nei mercati audiovisivi.

Negli ultimi anni, d’altra parte, le dinamiche di mercato nel settore dei media hanno evidenziato che la frammentazione (*rectius* divergenza) normativa che caratterizza gli Stati membri dell’Ue relativamente ai regimi di tutela del pluralismo rappresenta un chiaro ostacolo alla realizzazione degli obiettivi del mercato unico digitale. A questo riguardo, nella relazione di valutazione di impatto della regolazione, allegata alla proposta di regolamento recante lo *European Media Freedom Act* (di seguito, EMFA)¹⁰, è descritto un quadro molto frastagliato delle discipline nazionali. Secondo la relazione, ciò scoraggia investimenti e iniziative imprenditoriali nei mercati nazionali in ragione dell’incertezza sul diritto applicabile nei diversi mercati e di conseguenza crea alti costi amministrativi e di conformità per i fornitori di servizi media¹¹.

In questo contesto, dove i criteri di valutazione dell’impatto di una concentrazione sul pluralismo

6. Sul pluralismo dell’informazione come motivo imperativo di interesse generale nel diritto europeo, si veda MASTROIANNI 2013.

7. Un percorso caratterizzato da una progressiva armonizzazione e considerazione delle evoluzioni tecnologiche e di mercato, passando dalla direttiva “Televisione senza frontiere” del 2005 alla Direttiva SMAV 2010/13/UE, modificata da ultimo con Direttiva (UE) 2018/1808.

8. Si fa riferimento, in particolare, al principio di “*structural pluralism*” declinato nelle raccomandazioni del Consiglio d’Europa, in un sistema di tutela dove «Member states should seek to ensure that a sufficient variety of media outlets provided by a range of different owners, both private and public, is available to the public, taking into account the characteristics of the media market, notably the specific commercial and competition aspects». Council of Europe, Recommendation CM/Rec(2007)2 of the Committee of Ministers to member States on media pluralism and diversity of media content, I, 1.1.

9. BLEYER-SIMON-BROGI-CARLINI et al. 2024, p. 53.

10. Regolamento (UE) 2024/1083 del Parlamento europeo e del Consiglio dell’11 aprile 2024 che istituisce un quadro comune per i servizi di media nell’ambito del mercato interno e che modifica la direttiva 2010/13/UE (Regolamento europeo sulla libertà dei media). L’adozione del regolamento fa seguito alla proposta legislativa della Commissione del 16 settembre 2022, pubblicata nell’ambito delle iniziative pianificate dallo *European Democracy Action Plan* del dicembre 2020.

11. L’elevata frammentarietà dei regimi giuridici nazionali in Europa circa la tutela del pluralismo è stata oggetto anche di uno precedente studio della Commissione *Study on media plurality and diversity online* (maggio 2022) che evidenzia tali problemi di funzionamento del mercato interno dei servizi di media audiovisivi, i quali non consentono di tutelare adeguatamente i media a livello nazionale da interferenze sulla libertà editoriale.

e le competenze delle diverse autorità nazionali sono molto differenziati da Stato a Stato, non sempre è stato facile garantire che il pluralismo sia effettivamente perseguito e che le regole e gli scrutini nazionali non siano usati per limitare la libertà di stabilimento di altre imprese di media¹². Peraltro, se nel diritto europeo vi è una consolidata giurisprudenza sull'ammissibilità di deroghe alle libertà economiche e alla concorrenza, giustificate dalla tutela del pluralismo quale motivo di interesse generale, la stessa giurisprudenza esclude categoricamente che tali deroghe possano sostanzarsi in regole e procedure applicate in modo sproporzionato o discriminatorio e tradursi, quindi, in ostacoli al buon funzionamento del mercato interno, come dimostrano alcuni casi "storici" del diritto dei media audiovisivi¹³.

Un esempio, recente ed emblematico, in questo ambito è la nota vicenda giudiziaria italiana relativa all'operazione Vivendi-Mediaset. Tale vicenda è stata oggetto di una pronuncia della Corte di Giustizia Ue che ha palesato come una disciplina nazionale a tutela del pluralismo dei media possa effettivamente creare ostacoli ingiustificati alla libertà di stabilimento (e all'ingresso

in un mercato nazionale) alle imprese europee¹⁴. La sentenza ha quindi fornito inoppugnabili argomenti alla Commissione per proporre un intervento di armonizzazione che definisse un quadro comune di norme direttamente applicabili negli Stati membri, utilizzando come base giuridica l'articolo 114 TFUE. È stato proposto ed infine adottato un regolamento in luogo di una direttiva, seppur improntato a un approccio di "armonizzazione minima" ovvero "per principi" ed in un'ottica di proporzionalità¹⁵.

Una delle principali innovazioni normative introdotte nell'ordinamento europeo dall'EMFA è proprio la disciplina della valutazione delle concentrazioni del mercato dei media. Per la prima volta, quindi, un atto normativo europeo è intervenuto in una materia la cui armonizzazione si era sempre scontrata, da un lato, con la volontà degli Stati membri di mantenere intatte le proprie prerogative inerenti alla definizione (ed attuazione) delle politiche industriali (e culturali) nel settore audiovisivo e, dall'altro lato, con l'esistenza di tradizioni costituzionali differenziate con riguardo ai contenuti e ai sistemi di tutela del valore del pluralismo¹⁶.

12. Tra gli esempi riportati dalla Commissione, anche nel *Rule of Law Report*, vi è il tentativo di approvare una legge in Polonia per vietare la proprietà maggioritaria dei media radiotelevisivi da parte di società straniere che, seppur fallito per effetto del potere di veto del Presidente polacco, ha tuttavia trovato sostanziale attuazione nella decisione del regolatore nazionale dei media che ha di fatto impedito l'acquisizione. *Rule of Law Report 2021, Country Chapter on the rule of law situation in Poland (SWD(2021) 722)*. A proposito del caso ungherese, si veda BROGI-NENADIC-VIOLA DE AZEVEDO CUNHA-PARCU 2019.

13. Nella "storica" sentenza *Centro Europa 7*, ad esempio, la Corte di Giustizia dichiarò la normativa italiana in merito all'attribuzione delle frequenze in contrasto con la libertà di stabilimento nella misura in cui i relativi procedimenti non garantivano l'applicazione di criteri obiettivi, trasparenti, non discriminatori e proporzionati. Per un commento, si v. CAVALIERE 2008.

14. CGUE, causa C-719/18, *Vivendi SA v Autorità per le Garanzie nelle Comunicazioni*.

15. L'articolo 114 TFUE conferisce competenza all'UE per il "ravvicinamento" delle disposizioni legislative e regolamentari degli Stati membri per il buon funzionamento del mercato interno, lasciando discrezionalità alla Commissione nella scelta delle misure di armonizzazione (regolamenti o direttive) purché sia rispettata la proporzionalità in rapporto agli obiettivi perseguiti che, nel caso del mercato unico digitale, investono soprattutto i diritti dei consumatori. Analogo approccio normativo è rinvenibile nelle recenti misure di armonizzazione che hanno definito la cornice normativa di riferimento dell'economia digitale europea, trasversalmente ai mercati dei servizi di media: *Digital Service Act*, *Digital Markets Act*, *AI Act*, *Data Governance Act* e *Data Act*.

16. L'adozione dell'EMFA è stata infatti connotata da un acceso dibattito istituzionale sui profili di sussidiarietà e proporzionalità dell'intervento di armonizzazione, soprattutto da parte di alcuni Stati membri che si opponevano all'adozione di un sistema unitario di tutela del pluralismo e dell'indipendenza dei media, anche sulla base di un possibile contrasto di questo con l'art. 167(5) TFUE, che vieta azioni di armonizzazione normativa per quanto concerne gli "aspetti culturali" dei servizi media. In particolare, il Parlamento tedesco ha attivato

La disciplina in parola è collocata nella sezione 5 (artt. 21-23) del regolamento e stabilisce un nuovo quadro normativo di riferimento per l'adozione di misure nazionali che possano incidere «sul pluralismo dei media o sull'indipendenza editoriale dei fornitori di servizi di media», dettando a tal fine regole sostanziali e procedurali che entreranno in vigore l'8 agosto 2025. L'articolo 22, in particolare, impone agli Stati membri di adeguare il proprio ordinamento al fine di assicurare una valutazione delle concentrazioni del mercato dei media che potrebbero avere un impatto significativo sul pluralismo mediatico e sull'indipendenza editoriale. A tal fine, il comma 1 lett. a) di tale articolo prescrive agli Stati membri di improntare le discipline nazionali della valutazione di impatto sul pluralismo ai canoni di trasparenza, oggettività, proporzionalità e non discriminazione. Inoltre, la disciplina procedimentale della valutazione deve garantire il rispetto di termini adeguati alla garanzia della certezza del diritto (lett. e)). Altro elemento ricorrente nella giurisprudenza citata è, infatti, che l'incertezza connessa ad una insoddisfacente disciplina procedimentale vada ad incidere negativamente sulle scelte di investimento degli operatori di mercato.

2. Il "pluralismo" informativo e i suoi indicatori nell'attività di controllo delle concentrazioni

La forte frammentazione che caratterizza la disciplina delle operazioni di concentrazione nei mercati dei media, a fini di tutela del pluralismo, si

riscontra, in alcuni Stati, nella totale assenza di un regime giuridico specifico e, negli altri Stati, nella definizione di differenziate limitazioni sostanziali a garanzia della *market plurality*. Le legislazioni nazionali esistenti prevedono, infatti, variegati limiti alla proprietà basati sulla copertura delle audience o sulle quote di mercato, e/o restrizioni al controllo del capitale e/o restrizioni alla proprietà incrociata dei media¹⁷.

Proprio in ragione dell'ampia varietà di significati che il pluralismo dei media ha finora assunto e della varietà di strumenti adottati a sua tutela nei diversi contesti nazionali, la nuova disciplina recata dall'articolo 22 comma 2 si propone di uniformare criteri e metodologie di valutazione dell'impatto sul pluralismo delle operazioni di concentrazione. In particolare, il considerando 64 del regolamento EMFA specifica che, ai fini del controllo sulle concentrazioni, il pluralismo dei media dovrebbe essere inteso come «la possibilità di avere accesso a una varietà di servizi di media e contenuti mediatici che trasmettano opinioni, voci e analisi diverse».

È intuitivo come tale accezione richieda una valutazione distinta e autonoma rispetto alla mera analisi della concorrenzialità nei mercati, né essa può essere limitata alla verifica del rispetto di soglie quantitative fissate *ex lege* o di altri indici normativi predeterminati, richiedendo piuttosto un accertamento caso per caso delle specifiche circostanze che possono incidere sul valore del pluralismo informativo¹⁸.

una procedura di raccordo parlamentare contestando alla Commissione la violazione delle prerogative statali e dei principi di sussidiarietà e proporzionalità per effetto della scelta dell'articolo 114 TFUE come base giuridica dell'intervento di armonizzazione. Nell'ambito delle procedure parlamentari, la maggioranza delle assemblee legislative nazionali si è tuttavia espressa favorevolmente alla proposta EMFA, compreso il Parlamento italiano che si è espresso favorevolmente con un parere di conformità rilasciato ai sensi dell'articolo 5 TFUE. A questo riguardo, è bene sottolineare che il perseguimento di un corretto funzionamento del mercato interno dei servizi media non implica affatto una omogeneizzazione culturale e dei contenuti. Al contrario, in un ambito di concorrenza con i servizi digitali, un'armonizzazione delle condizioni ed una possibile estensione e consolidamento dei servizi devono essere associati ad una maggiore differenziazione dell'offerta, quantomeno su base nazionale e regionale. Per questo motivo, il regolamento EMFA non contrasta affatto con l'art. 167(5) TFUE.

17. Ad esempio, il sistema francese condiziona il rilascio delle licenze nel settore radiotelevisivo alla verifica di soglie quantitative fissate *ex lege* per prevenire la concentrazione dei media e i possibili impatti negativi sul pluralismo. Al contrario, in Irlanda non esistono soglie dimensionali per la proprietà, ma il divieto di avere il controllo o interessi sostanziali in un numero "eccessivo" di servizi di radiodiffusione sonora, o una "quantità eccessiva" di media di comunicazione in una determinata area geografica o di mercato.

18. In tal senso, come vedremo più diffusamente in seguito, si è pronunciata la Corte di Giustizia nella sentenza *Vivendi-AGCOM*, cit. para. 79 rilevando l'inidoneità della legge italiana (articolo 43 comma 11 TUSMA) a

Il principio generale è che la normativa orizzontale¹⁹ sulla concorrenza e la sua applicazione, rivolte a tutelare le corrette dinamiche concorrenziali, non sono sufficienti per valutare un impatto delle concentrazioni sul pluralismo, in ragione del fatto che quest'ultimo richiede una considerazione di diritti fondamentali (diritto all'informazione) inerenti al corretto svolgimento del processo democratico. È necessaria quindi una valutazione specifica che integri (ma non sostituisca) l'applicazione del diritto della concorrenza, per valutarne una più ampia (in)desiderabilità sociale.

Questa non sufficienza del diritto della concorrenza si sostanzia, in prima istanza, sotto un profilo quantitativo, ossia nel senso che una diminuzione della pressione concorrenziale che potrebbe essere considerata accettabile in altri mercati, molto probabilmente potrebbe non esserlo in quello dei media, in ragione degli "interessi pubblici" e "diritti fondamentali" coinvolti. Tale insufficienza ha anche un profilo qualitativo, ossia la valutazione a fini di pluralismo non può essere limitata ai soli aspetti di mercato. Infatti, l'esistenza di una pluralità di fornitori di contenuti mediatici e informativi non garantisce di per sé l'offerta di un'informazione diversificata e pluralistica e, soprattutto, non garantisce il diritto dei destinatari dei servizi di media ad «avere accesso a una pluralità di contenuti mediatici editorialmente indipendenti a beneficio di un dibattito libero e democratico» (art. 3 EMFA).

L'art. 22.2 del regolamento stabilisce in modo generale i principi in base ai quali dovrà essere attuato il *media plurality test*. Questi sono: a) l'impatto sul pluralismo, compresi gli effetti sulla formazione dell'opinione pubblica e sulla diversità dei servizi e dell'offerta dei media sul mercato, tenendo conto dell'ambiente online e degli interessi, dei legami o delle attività delle parti in altre imprese del settore dei media o di altri settori²⁰; b) l'esistenza

di salvaguardie per l'indipendenza editoriale; c) la sostenibilità economica delle imprese coinvolte nella concentrazione in assenza di concentrazione.

Si nota che tali criteri non aderiscono ad un mero concetto di "pluralismo esterno".

Innanzitutto, il regolamento, nella valutazione dell'impatto sul pluralismo, pone specifico accento su «gli effetti sulla formazione dell'opinione pubblica», che, come detto, non può essere limitata ai soli aspetti di mercato relativi alla quantità di fornitori di contenuti mediatici ed informativi.

Inoltre, nella disposizione normativa descritta, così come in tutto il regolamento, c'è una costante e stretta connessione fra i concetti e gli obiettivi di pluralismo dei media, da un lato, e di indipendenza editoriale, dall'altro lato. Pertanto, si può sostenere che «la riduzione di opinioni divergenti all'interno di quel mercato come conseguenza della concentrazione» (considerando 64) deve essere interpretata non solo in relazione alle quote di mercato e all'audience, ma anche prendendo in considerazione (sia in positivo sia in negativo) il modo in cui opera il fornitore di media coinvolto e la dipendenza dei contenuti editoriali dall'influenza dei proprietari.

Questa connessione fra pluralità nel mercato e indipendenza editoriale sembra sfumare la netta distinzione, concettuale ed applicativa, fra le dimensioni esterna e interna del pluralismo dei media, creando una interdipendenza (mobile). Coerentemente, la valutazione delle concentrazioni consisterà in un'analisi congiunta di tali aspetti, dove una riduzione del pluralismo esterno potrebbe essere controbilanciata da garanzie rafforzate di pluralismo interno – possibilmente definite anche da «impegni che le parti coinvolte nella concentrazione del mercato dei media possono offrire per salvaguardare il pluralismo dei media e l'indipendenza editoriale», art. 22.2 e)²¹.

garantire un'effettiva tutela del pluralismo «giacché fissa soglie che, non consentendo di determinare se e in quale misura un'impresa sia effettivamente in grado di influire sul contenuto dei media, non presentano un nesso con il rischio che corre il pluralismo dei media».

19. Ossia applicata indistintamente a tutti i settori industriali.

20. Ciò è in linea con la sentenza della CGUE nella causa *Vivendi SA*, dove è affermato che il superamento di soglie basate esclusivamente sulle quote di mercato non è sufficiente a dimostrare una riduzione del pluralismo.

21. Ad esempio, un'acquisizione da parte di un fornitore di servizi media con una linea editoriale "x" da parte di un fornitore di servizi media con una linea editoriale "y", nel caso l'operazione abbia un impatto problematico sotto un profilo di pluralismo esterno, potrebbe essere teoricamente valutata non negativamente in ragione di impegni a non alterare la linea editoriale "x" esistente.

In ogni caso, i criteri definiti all'art. 22.2 rappresentano di per sé norme di principio ovvero concetti giuridici indeterminati che necessitano di una attività di specificazione, che il regolamento richiede ancor prima dell'attività di interpretazione delle autorità nazionali chiamate a darne attuazione. A fini di certezza del diritto, è infatti previsto che la Commissione integri il significato delle disposizioni con proprie linee guida. Tali orientamenti saranno facilmente modificabili (a discrezione della Commissione stessa) al fine di tenere in pronta considerazione le repentine evoluzioni nell'ambiente digitale dei media.

Gli orientamenti della Commissione avranno il compito non solo di dettagliare il significato dei principi generali contenuti nel regolamento, ma anche di specificare in che rapporto sono gli uni con gli altri. Questo aspetto è rilevante in funzione del menzionato rapporto di potenziale complementarità fra i concetti di pluralismo ed indipendenza editoriale, ma anche in funzione del fatto che il principio della sostenibilità economica è contro-tendente rispetto ai primi due, e quindi il loro bilanciamento e/o prioritizzazione possono avvenire in svariate (dinamiche) modalità. Ad esempio, come accennato, se una fusione è giustificata da ragioni di sostenibilità economica, ma comporta rischi sostanziali di riduzione del pluralismo esterno, potrebbe essere possibile/necessario richiedere e applicare una serie di garanzie rafforzate in termini di indipendenza editoriale, diversità dei contenuti e pluralismo interno.

Un altro concetto fondamentale che gli orientamenti dovranno chiarire è cosa si intenda con la locuzione "tenendo in conto l'ambiente online": è, infatti, sotto un profilo sostanziale, fondamentale considerare oggi il ruolo delle piattaforme online sul pluralismo informativo, anche per valutare la concentrazione di potere che influisce sull'opinione pubblica.

Peraltro, sotto un profilo di campo di applicazione, le concentrazioni che coinvolgono piattaforme online sono incluse nell'ambito di questo articolo, nel caso in cui sia coinvolto almeno un fornitore di servizi media o la piattaforma stessa

fornisca "accesso" a contenuti mediatici (art. 2 n. 15 EMFA).

La disciplina delle concentrazioni dei media ricomprende quindi le piattaforme online tra i soggetti obbligati a notificare operazioni di concentrazione alle ANR nella misura in cui tali soggetti forniscano accesso ai contenuti mediatici. Risulterà quindi cruciale definire il perimetro del concetto di "accesso", che dato il contesto sostanziale sembra potersi interpretare in modo estensivo.

In questo contesto, sembra peraltro che la "considerazione dell'ambiente online" non possa non portare con sé elementi conglomerati nella valutazione delle concentrazioni, sia appunto per come è oggi strutturato il sistema dei media, sia in ragione del fatto che la valutazione di impatto sul pluralismo non è di per sé connessa con la definizione di mercati rilevanti e non si appiattisce sulla valutazione di impatto concorrenziale.

Quindi, il regolamento EMFA attua una "estensione" del settore dei media e le piattaforme online sono destinatarie di un regime di obblighi differenziato a seconda dell'effettiva rilevanza o influenza dei servizi offerti rispetto all'accesso ai contenuti mediatici, così come ai problemi legati alla diffusione degli stessi per effetto di fenomeni di amplificazione, polarizzazione e disinformazione²², nonché agli squilibri di mercato legati agli sviluppi tecnologici nell'*online advertising* e alle asimmetrie nella misurazione delle audience.

In questo senso, un aspetto cruciale da tenere in considerazione nell'ambiente online e nell'attività di intermediazione dell'accesso a contenuti mediatici e/o informativi delle piattaforme che usano meccanismi di selezione algoritmica è quello del "pluralismo interno dal lato della domanda", che anch'esso è basato su una sfumatura della distinzione dei concetti di pluralismo esistenti, in ragione del mutato contesto di mercato²³.

In altri termini, sembra necessario nella valutazione delle concentrazioni tenere in considerazione anche il generale impatto (negativo) prodotto dalle fonti algoritmiche sulla «possibilità di avere accesso a una varietà di servizi di media e contenuti mediatici che trasmettano opinioni, voci e

22. Tali aspetti hanno inoltre richiesto una disciplina specifica a garanzia di un corretto bilanciamento tra libertà di informazione e moderazione dei contenuti da parte degli intermediari designati come *very large online platforms* ai sensi del *Digital Service Act* (artt. 18 e 19 EMFA).

23. MANGANELLI 2023.

analisi diverse». Infatti, nel risolvere efficientemente il “sovraccarico informativo” tipico dell’ambiente online (dove l’offerta è tutt’altro che scarsa) e soddisfare le preferenze degli utenti, la personalizzazione algoritmica in ambito di contenuti informativi e medialità necessariamente contribuisce a creare ed amplificare le notorie “camere d’eco digitali”. Ossia, ciò che la piattaforma propone è ciò che l’utente (già) preferisce, la sua esistente visione del mondo, che ha rivelato (direttamente o indirettamente) alla piattaforma ed in cui essa, in qualità di porta di accesso all’informazione (*information gatekeeper*) lo ha “efficientemente” relegato²⁴. Pluralismo informativo, invece, anche nell’accezione del regolamento EMFA, è una *diversity exposure*, ossia significa essere sottoposti potenzialmente anche a contenuti informativi sui quali si potrebbe attualmente essere in disaccordo, ma sui quali si deve avere comunque la possibilità di fare una scelta, potenzialmente reversibile nel tempo²⁵.

3. La valutazione di impatto sul pluralismo come nuova funzione regolatoria nel sistema di governance dei media

Il regolamento EMFA attribuisce alla Commissione, con il supporto di un nuovo organismo di raccordo delle autorità nazionali, lo *European Board of Media Services* (EBMS), rilevanti poteri di intervento nelle decisioni delle autorità nazionali competenti in materia di controllo sulle concentrazioni.

L’obiettivo di superamento della frammentazione nazionale, che rappresenta la motivazione primaria per l’intervento legislativo europeo, ha

infatti richiesto anche la definizione armonizzata di nuovi assetti organizzativi delle autorità preposte all’assolvimento delle funzioni di controllo delle concentrazioni dei media e di un nuovo sistema di governance istituzionale, comprendente il coordinamento “verticale” con la Commissione e lo EBMS ed anche gli eventuali rapporti “orizzontali” con le autorità di concorrenza.

Partendo da quest’ultimo aspetto, il comma 1 lett. c) dell’articolo 22 impone agli Stati membri di designare le “autorità o gli organismi nazionali di regolamentazione” – puntualmente definite all’articolo 7 EMFA – quali soggetti nazionali responsabili della valutazione o di garantirne comunque il coinvolgimento sostanziale di queste nella valutazione. Il comma 1 dell’articolo 22 sancisce quindi l’autonomia oggettiva (e tendenzialmente anche soggettiva) della funzione di tutela del pluralismo rispetto alla tutela della concorrenza²⁶.

La norma mira, pertanto, ad affidare la valutazione di impatto sul pluralismo alle “autorità indipendenti per i media” o a “organismi nazionali indipendenti” a cui gli Stati membri abbiano già affidato la funzione di “Autorità Nazionale di Regolamentazione” (ANR) per l’attuazione della Direttiva (UE) sui servizi di media audiovisivi (SMAV), ribadendone i requisiti sia funzionali sia organizzativi di autonomia e indipendenza (ed espressamente richiamando l’esigenza di un’adeguata dotazione di risorse che gli Stati membri sono tenuti a garantire).

Pur riservando il *media plurality test* a tali soggetti, l’articolo 22 EMFA lascia tuttavia discrezionalità agli Stati membri nella disciplina nazionale

24. Per maggior approfondimento su questi concetti si rimanda a MANGANELLI–NICITA 2022.

25. In questo senso e con questo obiettivo, si potrebbe interpretare la disposizione di cui all’art. 20 EMFA concernente il diritto alla personalizzazione dell’offerta di media audiovisivi. Sebbene tale norma sia stata concepita per le interfacce degli apparati di ricezione, l’art. 20 potrebbe interpretarsi estensivamente, conferendo agli utenti delle grandi piattaforme digitali il diritto «di modificare facilmente le impostazioni predefinite di qualsiasi dispositivo o interfaccia utente che controlla o gestisce l’accesso ai servizi di media audiovisivi e il loro utilizzo, al fine di personalizzare l’offerta di media audiovisivi in base ai loro interessi o preferenze, nel rispetto della legge». Ciò consentirebbe di aumentare la *diversity exposure* di un utente indipendentemente dalle preferenze attuali rivelate e rendere così potenzialmente possibile l’ampliamento o la modifica nel tempo delle sue preferenze, al fine di reintrodurre una effettiva libertà di scelta fra una molteplicità di fonti (o tipi di fonti) alternative.

26. «La valutazione delle concentrazioni del mercato dei media di cui al presente paragrafo è distinta da quelle a norma del diritto della concorrenza dell’Unione e nazionale, comprese quelle previste dalle norme sul controllo delle concentrazioni. Essa non pregiudica l’articolo 21, paragrafo 4, del regolamento (CE) n. 139/2004, ove applicabile». Art. 22 comma 1.

dei procedimenti di controllo sulle operazioni di concentrazione e sul relativo assetto delle competenze. La valutazione di impatto sul pluralismo potrà quindi assumere la forma di parere vincolante dell'autorità dei media nell'ambito di un procedimento principale di competenza dell'autorità per la concorrenza, oppure svolgersi in via del tutto autonoma e indipendente essendo oggetto di una distinta funzione di vigilanza attribuita all'autorità nazionale di regolamentazione, come avviene in Italia.

Ferma restando la discrezionalità degli Stati membri nella disciplina dei rapporti tra autorità della concorrenza e autorità di regolazione dei media, l'attribuzione alle ANR della funzione di valutazione di impatto sul pluralismo non è, in ogni caso, priva di effetti sulle discipline procedurali nazionali. Allo stato attuale, infatti, diversi Stati membri dispongono di sistemi che consentono ai Ministeri o agli organismi governativi di intervenire nei procedimenti di controllo delle concentrazioni e di annullare le decisioni delle autorità nazionali competenti per motivi diversi dalla tutela della concorrenza, che vanno dalla protezione del pluralismo dei media alla salvaguardia della sicurezza pubblica o di altri interessi generali. Con l'entrata in vigore dell'articolo 22 EMFA, la funzione di tutela del pluralismo dei media è sottratta all'intervento governativo e riservata alle autorità indipendenti, rendendo, pertanto, contrarie al regolamento le discipline che mantengano prerogative delle autorità di governo per le operazioni di concentrazione nel settore dei media.

La garanzia di una valutazione indipendente è stata fortemente perorata dall'organismo europeo dei regolatori dei media ERGA – che ha contribuito attivamente al negoziato sulla proposta EMFA e, con specifico riguardo alla valutazione di impatto del pluralismo, segnalato l'importanza di assicurare la facoltà di un intervento autonomo nei procedimenti di controllo sulle concentrazioni anche al nuovo Board delle ANR.

In effetti, se a livello nazionale l'attribuzione della competenza alle ANR assicura indipendenza e terzietà alla valutazione di impatto del pluralismo in un mercato, quello dei media, ancora fortemente connotato da partecipazioni statali negli

assetti proprietari e da altre forme di controllo diretto sulla governance e la fornitura dei servizi di media (in virtù della titolarità del servizio pubblico di media), l'indipendenza del Board in questa materia (art. 9 EMFA) assicura un temperamento rispetto alle iniziative della Commissione ai fini di un bilanciamento complessivo tra le istanze nazionali e le finalità generali del diritto euronitario che formano la cornice giuridica e istituzionale in cui si svolge l'attività di mero accertamento tecnico “neutrale”²⁷.

Anche grazie alle proposte emendative di ERGA, la disciplina procedimentale della valutazione di impatto sul pluralismo è stata quindi rimodulata rispetto alla proposta legislativa originaria, con la previsione, all'articolo 23 EMFA, di un autonomo potere di iniziativa del Board in materia di controllo sulle concentrazioni che non siano state previamente notificate (al Board e alla Commissione) in quanto suscettibili di incidere sul funzionamento del mercato interno dei media.

In particolare, da un lato, le ANR sono tenute a consultare il Board sulle operazioni di concentrazione del mercato dei media che «possano incidere sul funzionamento del mercato interno» nel settore mediatico, notificando previamente il progetto di valutazione o di provvedimento al fine di acquisirne il parere. Dall'altro lato, in assenza di una richiesta in tal senso, il Board di propria iniziativa o su richiesta della Commissione, elabora un parere sull'impatto di una concentrazione sul pluralismo e sull'indipendenza editoriale, qualora ritenga che tale concentrazione possa incidere sul funzionamento del mercato interno dei servizi di media. Tale parere dovrà fondarsi su criteri sostanziali fissati da EMFA o dalle linee guida della Commissione che, a sua volta, può intervenire con proprio parere sulle misure adottate dalle ANR che possono incidere sui fornitori di media e che devono essere obbligatoriamente comunicate ai sensi dell'articolo 21 del regolamento.

Le ANR designate per la valutazione delle concentrazioni a tutela del pluralismo sono altresì responsabili per la procedura di notifica e la definizione dei relativi criteri. Ai sensi dell'articolo 2 comma 1 lett. b) EMFA le norme nazionali impongono obblighi di notifica delle «concentrazioni

27. Sulle motivazioni economiche e giuridico-istituzionali della “regolazione indipendente” si rimanda a MANGANELLI–NAPOLITANO 2024.

del mercato dei media» definite attraverso un rinvio alla definizione generale di “concentrazione” recata dall’articolo 3 del citato regolamento sulle concentrazioni (CE) n. 139/2004, laddove la concentrazione «interessa almeno un fornitore di servizi di media o un fornitore di una piattaforma online che fornisce accesso a contenuti mediatici» (art. 2 n. 15).

L’ambito di applicazione soggettivo della norma estende pertanto la valutazione di impatto sul pluralismo a un paniere di servizi più ampio di quello identificato dalla definizione di “servizi di media” del Regolamento EMFA che, a sua volta, ricomprende un numero di attività maggiore di quelle individuate dalla direttiva SMAV, poiché riguarda «qualsiasi mezzo» utilizzato per la fornitura al grande pubblico e dietro corrispettivo di «programmi o di pubblicazioni di carattere giornalistico, sotto la responsabilità editoriale di un fornitore di servizi di media (...) al fine di informare, intrattenere o istruire». In virtù di questa nuova definizione, i servizi di media abbracciano quindi anche il settore della stampa, i podcast audio, i giornalisti e professionisti che pubblicano dietro corrispettivo contenuti di media (quindi anche i *vloggers*) e, come menzionato, le piattaforme online, che si aggiungono al novero di soggetti e attività economiche già disciplinati dalla direttiva SMAV che resta, in ogni caso, il quadro normativo speciale applicabile ai servizi di media audiovisivi²⁸.

4. L’implementazione a livello nazionale: la disciplina del TUSMA e la sua recente evoluzione

In coerenza con gli altri plessi di riforma legislativa adottati in attuazione della *Strategia europea per l’economia digitale*, il regolamento EMFA mira a garantire il buon funzionamento del mercato

interno dei servizi media con misure di ravvicinamento che facciano salve le legislazioni nazionali compatibili, purché finalizzate a stabilire o mantenere livelli più elevati di tutela del pluralismo dei media o dell’indipendenza editoriale.

In particolare, a fronte di diritti e obblighi direttamente azionabili per i fornitori di servizi di media, l’articolo 1 comma 3 EMFA lascia impregiudicata la potestà normativa degli Stati membri di mantenere o adottare regole più dettagliate o più rigorose in taluni ambiti di intervento, tra cui il capo III che si limita, pertanto, a dettare le “prescrizioni” (principi, criteri e requisiti) a cui gli Stati membri dovranno attenersi nel porre in essere misure e procedure per il buon funzionamento del mercato dei media, tra cui figurano le disposizioni sulla valutazione delle concentrazioni.

L’implicazione giuridica di questo approccio normativo è, pertanto, una sostanziale attenuazione dell’efficacia diretta, tratto tipico dello strumento regolamentare nel diritto europeo, e la possibilità/necessità di predisporre una legislazione nazionale di attuazione delle disposizioni EMFA, lasciando quindi inevitabilmente qualche margine di discrezionalità agli Stati membri. Sarà quindi importante ed ancor più interessante andare a valutare la compatibilità delle legislazioni nazionali esistenti con il nuovo regolamento anche con riferimento agli orientamenti che la Commissione è chiamata ad adottare per dare piena attuazione al *market plurality test*.

Per quanto concerne l’ordinamento italiano, come noto, è vigente una disciplina specifica sulle concentrazioni e sulla valutazione del pluralismo informativo nel sistema integrato delle comunicazioni (SIC). Queste norme erano recate dall’art. 43 (“Posizioni dominanti nel sistema integrato delle comunicazioni”) del d.lgs. 177/05 (TUSMAR)²⁹, poi confluite nel nuovo “Testo Unico dei servizi

28. I considerando 9 e 10 EMFA chiariscono puntualmente che la nuova definizione di “servizi di media” fa riferimento alle trasmissioni televisive o radiofoniche su richiesta, ai servizi di media audiovisivi, podcast audio o pubblicazioni di carattere giornalistico, mentre sono esclusi i contenuti generati dagli utenti caricati su un sito online, a meno che non costituiscano un’attività professionale con corrispettivo, sia esso di natura finanziaria o di altra natura (in tal senso, si evidenzia che l’EMFA fa rientrare nella definizione di servizi di media anche i c.d. “vloggers”). Sono escluse la corrispondenza privata (ad es., la posta elettronica) e tutti i servizi che non hanno quale scopo principale la fornitura di programmi audiovisivi o audio o pubblicazioni a stampa, ovvero quando il contenuto è meramente accessorio rispetto al servizio. Alcune disposizioni, poi, si applicano alle *very large online platform* (di seguito “VLOPs”), in linea con le previsioni del DSA.

29. Testo unico dei servizi di media audiovisivi e radiofonici (d.lgs. 31 luglio 2005) il cui comma 11 è stato dichiarato incompatibile con il diritto euronitario e, in particolare, con l’articolo 49 TFUE.

di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato" (TUSMA) che ha introdotto disposizioni innovative in materia all'art. 51 ("Posizioni di significativo potere di mercato lesive del pluralismo nel sistema integrato delle comunicazioni")³⁰.

Sul confronto fra la legislazione nazionale vigente ed il nuovo regolamento EMFA, è cruciale osservare come la sentenza *Vivendi-Mediaset*, che ha concorso all'adozione di EMFA, ha dato primario impulso anche alla riforma della disciplina italiana a tutela del pluralismo³¹. Anche in virtù di questo parallelismo, pertanto, negli ultimi anni, la legislazione italiana in materia di concorrenza e pluralismo nel settore dei media ha rappresentato per la Commissione un punto di osservazione di alcune problematiche emerse.

In effetti, l'attuale disciplina del TUSMA sembra sostanzialmente conforme ai requisiti organizzativi e procedurali richiesti dalla disciplina eurolunitaria, richiedendo solo minimi aggiustamenti al sistema di governance. Questa, infatti, come descritto, affida alle ANR, in quanto autorità indipendenti dei media, la valutazione dell'impatto sul pluralismo e sull'indipendenza editoriale dei media quale funzione autonoma dai procedimenti in materia di concorrenza. Su questo aspetto, il TUSMA, all'articolo 9, affida all'Autorità per le garanzie nelle comunicazioni (AGCOM) – già competente per i procedimenti di controllo sulle concentrazioni nei media e per la valutazione e verifica di posizioni dominanti a tutela del pluralismo nel SIC – la

funzione di ANR ai sensi della direttiva SMAV e, quindi, automaticamente il ruolo di "autorità per i media" ai sensi dell'articolo 7 EMFA nel rispetto dei requisiti di indipendenza, imparzialità e trasparenza richiesti dal diritto europeo e richiamati dal Testo unico.

Come accennato, quindi, la valutazione di impatto sul pluralismo si svolge in Italia in via del tutto autonoma e indipendente rispetto a una valutazione dell'Autorità di concorrenza, cui la legge italiana non affida neanche un potere consultivo. La scelta del legislatore italiano, risalente alla legge istitutiva dell'Autorità e confermata, da ultimo, con la nuova disciplina adottata nel 2021, opera quindi una netta separazione, sia oggettiva sia soggettiva, tra la funzione di verifica delle posizioni lesive del pluralismo affidata ad AGCOM e il controllo sulle concentrazioni a fini di tutela della concorrenza di competenza dell'Autorità garante per la concorrenza e il mercato³². Per quanto concerne i poteri di intervento a tutela del pluralismo, la legislazione italiana conferisce ad AGCOM il potere di rimuovere o impedire la formazione di posizioni di significativo potere di mercato lesive del pluralismo, attraverso misure sia comportamentali sia strutturali, anche rendendo vincolanti impegni presentati delle parti coinvolte, se ritenuti dall'Autorità sufficienti a eliminare o impedire il formarsi delle posizioni di significativo potere di mercato lesive del pluralismo³³.

Ovviamente, si dovrà invece dare attuazione al nuovo sistema di governance allargata previsto

30. Testo unico sui servizi di media audiovisivi (d.lgs. 28 novembre 2021, n. 208). Per un commento alla nuova disciplina dell'articolo 51 TUSMA, si veda GRANDINETTI 2022.

31. Si veda APA-AVVISATI 2023.

32. A tal riguardo, sembra interessante ricordare come, in Italia, la legge 287 del 1990 nella sua versione originaria prevedeva, al comma 1 dell'art. 20, competenze esclusive di tutela della concorrenza (intese, abusi di posizione dominante e controllo delle concentrazioni) per il Garante per la radiodiffusione e l'editoria, attribuendo ad AGCM un mero potere consultivo. L'attribuzione di competenze antitrust all'Autorità di regolazione, in caso di non completa convergenza degli interessi perseguiti, era tutt'altro che neutrale in quanto l'obiettivo di policy era proprio di bilanciare la tutela della concorrenza con i diversi ed ulteriori interessi che l'Autorità di regolazione doveva perseguire. Le competenze di applicazione diretta della legge 287 sono state successivamente attribuite all'Autorità di concorrenza, in quanto la legge 249 del 1997, istitutiva di AGCOM, ha assegnato al suo Consiglio tutte le competenze e le funzioni precedentemente affidate al Garante ad eccezione appunto delle competenze di tutela della concorrenza contenute al comma 1 dell'art. 20 della legge 287 che è stato abrogato. La stessa legge ha altresì conferito ad AGCOM un potere consultivo, non vincolante, nei procedimenti antitrust e di concentrazione dinanzi ad AGCM che coinvolgono "operatori del settore delle comunicazioni". Art. 1 comma 6 lett. c) n. 11 della legge 249 del 1997. MANGANELLI 2021.

33. Art. 51 comma 6, d.lgs. 8 novembre 2021, n. 208.

da EMFA, imperniato sulla cooperazione transfrontaliera tra regolatore nazionale, Board e la Commissione che comporterà, in particolare, un meccanismo di consultazione del Board e l'adozione di pareri del Board e della Commissione sulle concentrazioni che possano incidere sul funzionamento del mercato interno dei servizi di media.

Per quanto concerne, invece, gli aspetti sostanziali, rispetto al vecchio plesso normativo nazionale, il divieto di detenere posizioni di potere di mercato lesive del pluralismo di cui all'art. 51 TUSMA non diviene automaticamente operativo in corrispondenza di soglie prefissate, le quali non si configurano più come limiti anti-concentrativi il cui superamento è vietato³⁴. Infatti, si definiscono normativamente (alcune) situazioni di mercato sintomatiche di potenziali lesioni del pluralismo, il cui verificarsi innesca obblighi di comunicazione all'Autorità in capo a tutti quei soggetti, che, anche attraverso società controllate o società collegate ed anche a seguito di intese o di operazioni di concentrazione, si vengano a trovare o già si trovino in quelle situazioni.

La valutazione della lesività del pluralismo (che non si limita quindi al controllo delle concentrazioni ma si estende anche alle posizioni esistenti) è affidata poi all'accertamento caso per caso

dell'Autorità, sia in seguito alle notifiche di cui sopra, sia d'ufficio sulla base dei suoi accertamenti sull'evoluzione del sistema integrato delle comunicazioni (SIC)³⁵ e quello dei mercati che lo compongono, sia su segnalazione di chi vi abbia interesse (comma 5). L'Autorità nella sua valutazione tiene conto di specifici aspetti e dinamiche di mercato che possono incidere sul pluralismo informativo e che sono descritti allo stesso comma 5. Tali aspetti sono più numerosi rispetto al passato e riflettono in maniera più compiuta le specificità concorrenziali e pluralistiche degli attuali ecosistemi dei media, anche in un ambiente online³⁶.

Il passaggio dal divieto "rigido" di posizioni dominanti a quello "più duttile", caso per caso, di posizioni lesive del pluralismo attribuisce un nuovo significato operativo all'accertamento delle situazioni di potere economico individuali e collettive sia nel SIC sia nei singoli mercati che lo compongono. Se da un lato, infatti, la considerazione, a fini di tutela del pluralismo, di un ambito di mercato "integrato" ha anticipato ed è stata funzionale a considerare l'evoluzione digitale dei mercati dei media³⁷, dall'altro lato, tuttavia, questa estensione, in un quadro di limiti concentrativi prefissati e non rivolti (o parzialmente rivolti) ai singoli mercati, aveva diluito l'impatto potenzialmente lesivo

34. La revisione del meccanismo di soglie anti-concentrative prefissate previsto dall'articolo 43, comma 11, del TUSMAR è stata introdotta dal legislatore per dare attuazione alla sentenza della Corte di giustizia nel caso *Vivendi-Mediaset*, nella quale la Corte riteneva che esse non fossero idonee, sotto il profilo della proporzionalità, a garantire il pluralismo dei media. Queste, infatti, stabilivano soglie di mercato astratte che non consentivano di tenere in considerazione se e in quale misura un'impresa fosse effettivamente in grado di influire sul contenuto delle attività editoriali dei media.

35. Ossia «il settore economico che comprende le attività di stampa quotidiana e periodica, delle agenzie di stampa, di editoria elettronica, anche per il tramite di Internet, di radio e servizi di media audiovisivi e radiofonici, cinema, pubblicità esterna, sponsorizzazioni e pubblicità online», art. 3, comma 1, lett. z) TUSMA.

36. Si veda LUPU 2023.

37. Come riconosciuto anche dalla stessa AGCOM (delibera 94/23/CONS) i criteri individuati dal legislatore nell'art. 51, comma 5 del nuovo TUSMA riflettono la consapevolezza della trasformazione digitale e della progressiva affermazione delle grandi piattaforme online multinazionali in posizione di *gatekeeper* e della conseguente esigenza di adeguare le metodologie di analisi a «una visione evidentemente ecosistemica» del settore mediale, inteso in un'accezione ampia e di fatto allineato alla nozione estesa di media dell'EMFA. Ciò garantisce la possibilità di svolgere un'analisi di concorrenza non solo intra-mediale, ma anche inter-mediale, al di là dei singoli mercati rilevanti, sulla base di un ampio set di indicatori che comprende oltre alle quote di ricavi, la «convergenza fra settori e delle sinergie con altri mercati contigui» così come dei fenomeni di integrazione verticale e conglomerale nel settore audiovisivo, dove l'economia dei dati, ovvero la disponibilità e il controllo sugli stessi va assumendo crescente centralità (delibera n. 66/24/CONS, cit.).

dell'effettivo potere economico esercitato da alcuni attori tradizionali ed emergenti nel SIC³⁸. Il TUSMA, rimettendo all'Autorità, sulla base di criteri definiti, la verifica della presenza di posizioni lesive del pluralismo, consente una valutazione molto più penetrante anche nei singoli mercati che compongono il SIC³⁹.

Coerentemente con tale impianto e con l'EMFA, il nuovo TUSMA, sempre ai sensi dell'art. 51 comma 5, ha stabilito che, sulla base di criteri ivi definiti, l'Autorità definisca ex-ante la metodologia specifica per la verifica del rischio di lesione del pluralismo, mediante linee guida, che saranno oggetto di revisione periodica con cadenza almeno triennale. In questo modo, gli ampi criteri individuati dal legislatore trovano contestualizzazione in maniera dinamica nelle linee guida dell'Autorità, appagando la necessità sia di un loro rapido e continuo adattamento alle mutevoli situazioni di mercato, sia di una solida certezza del diritto che deve caratterizzare *ex ante* le norme a difesa del pluralismo (e non solo nel momento di attuazione delle disposizioni da parte dell'autorità)⁴⁰.

L'Autorità ha definitivamente adottato i suoi primi orientamenti, con la delibera 66/24/CONS, improntando la metodologia di analisi proposta alla peculiare declinazione del valore della concorrenza nell'art. 51 TUSMA quale strumento finalizzato alla tutela del pluralismo e al divieto di costituzione di posizioni di significativo potere di mercato di esso lesive. A tal fine l'autorità, oltre ai criteri "classici" di analisi di concorrenza, contempla indici specifici connessi alla diffusione di

informazione e programmi e declina il nuovo set di indicatori sia con riferimento alla caratterizzazione a più versanti dei mercati dei media sia estendendo l'analisi ai mercati degli input a monte (i.e., sul versante dei ricavi pubblicitari, in termini di audience raggiungibili e servizi abilitanti, alla luce soprattutto delle dinamiche caratterizzanti i mercati della pubblicità *data-driven*).

L'adattamento della metodologia di analisi concorrenziale alle finalità di tutela del pluralismo proposto da AGCOM nelle sue linee guida individua, pertanto, nuovi indici e parametri per lo scrutinio affidato alle autorità indipendenti dei media orientando la funzione di vigilanza sull'evoluzione dei mercati (e sulle concentrazioni) dei media alla specifica finalità di tutela dell'accesso alle fonti informative, rifacendosi in tale prospettiva la citata consolidata giurisprudenza costituzionale italiana sulla garanzia che «i soggetti portatori di opinioni diverse possano esprimersi senza il pericolo di essere emarginati a causa dei processi di concentrazione delle risorse tecniche ed economiche nelle mani di uno o di pochi»⁴¹.

Alla luce di questo nuovo impianto normativo, che innova il sistema di indicatori a tutela del pluralismo e chiarisce definitivamente l'estensione dell'ambito soggettivo ai nuovi attori del sistema dei media, anche le linee guida AGCOM possono probabilmente andare a rappresentare un modello di riferimento per la futura adozione degli orientamenti della Commissione ai fini del *market plurality test* richiesto dell'EMFA.

38. Si veda, ad esempio, il capitolo 9 di ZACCARIA-VALASTRO-ALBANESI 2023.

39. A questo riguardo sembra importante sottolineare che la più volte citata sentenza della Corte sul caso *Vivendi-Mediaset* non ha ritenuto incompatibile con il diritto Ue l'intero impianto del SIC ed il suo utilizzo a fini di tutela del pluralismo informativo (cfr. GRANDINETTI 2022), ma il suo uso in un contesto di limiti anti-concentrativi definiti che non tenessero in considerazione la distribuzione delle quote e del potere di mercato nei vari mercati che compongono il SIC. Valutazione che adesso l'Autorità ha il potere e la competenza di attuare.

40. Sull'importanza e gli effetti giuridici di "autovincolo" degli atti di soft law si rimanda a MORBIDELLI 2016: «a fronte del disvalore rappresentato dalla incertezza del diritto cui non può porre rimedio che in casi rarissimi la interpretazione autentica, mentre la giurisprudenza, quando non concorre anch'essa all'incertezza, è comunque una risposta non tempestiva, la soft law, ove provenga da soggetti dotati di autorevolezza, a mo' di ossimoro, è un non diritto che concorre alla certezza del diritto».

41. Corte Cost., sentenza n. 826 del 1988.

Riferimenti bibliografici

- E. APA, M. AVVISATI (2023), *La sentenza della Corte di giustizia Ue nel caso Vivendi e la revisione della disciplina italiana in materia di pluralismo*, in “Astrid Rassegna”, 2023, n. 11
- K. BLEYER-SIMON, E. BROGI, R. CARLINI et al. (2024), *Monitoring media pluralism in the digital era: application of the media pluralism monitor in the European member states and in candidate countries in 2023*, European University Institute (EUI), 2024
- E. BROGI, I. NENADIC, M. VIOLA DE AZEVEDO CUNHA, P.L. PARCU (2019), *Assessing certain recent developments in the Hungarian media market through the prism of the Media Pluralism Monitor*, European University Institute (EUI), July 2019
- C. CAMBINI, A. MANGANELLI, A. NICITA (2024), *Economia e regolazione delle reti e delle infrastrutture*, in C. Cambini, A. Manganelli, G. Napolitano, A. Nicita (a cura di), “Economia e diritto della regolazione”, il Mulino, 2024
- P. CAVALIERE (2008), *La Corte di giustizia dà ragione a Europa 7: Tra concorrenza e pluralismo, un nuovo slancio per il mercato televisivo italiano?*, in “Diritto pubblico comparato ed europeo”, 2008, n. 2
- O. GRANDINETTI (2022), *La tutela del pluralismo nel nuovo Testo unico sui servizi di media audiovisivi*, in “MediaLaws”, 2022, n. 2
- P. LUPI (2023), *Commento all’art. 51*, in C. Contessa, P. del Vecchio (a cura di), “Testo Unico Servizi Media Audiovisivi”, Editoriale Scientifica, 2023
- A. MANGANELLI (2023), *Piattaforme digitali e social network, fra pluralità degli ordinamenti, pluralismo informativo e potere di mercato*, in “Giurisprudenza costituzionale”, 2023, n. 2
- A. MANGANELLI (2021), *Il rapporto fra tutela della concorrenza e regolazione*, in V. Falce (a cura di), “Competition Law enforcement in digital markets”, Giappichelli, 2021
- A. MANGANELLI, G. NAPOLITANO (2024), *Regolazione, diritto e istituzioni*, in C. Cambini, A. Manganelli, G. Napolitano, A. Nicita (a cura di), “Economia e diritto della regolazione”, il Mulino, 2024
- A. MANGANELLI, A. NICITA (2022), *Regulating digital markets: the EU approach*, Palgrave Macmillan, 2022
- R. MASTROIANNI (2013), *La dimension europeenne de la regulation audiovisuelle: vers une nouvelle directive sur le pluralisme de l’information?*, in “Astrid Rassegna”, 2013, n. 17
- G. MORBIDELLI (2016), *Degli effetti giuridici della soft law*, in “Rivista della regolazione dei mercati”, 2016, n. 2
- R. ZACCARIA, A. VALASTRO, E. ALBANESI (2023), *Diritto dell’informazione e della comunicazione*, Cedam, 2023



TANJA KERŠEVAN

From rhetoric to regulation: EMFA and media concentration in the digital age

This article examines the evolving political discourse and practices surrounding media pluralism within the European Union (EU) in light of the European Media Freedom Act (EMFA), which mandates that Member States evaluate the impact of media market concentrations on media pluralism. Through analysis of key EU legislative and policy texts the article explores how media concentration is addressed, with a particular focus on two smaller Member States (Croatia and Slovenia) where outdated laws and the lack of data to assess media pluralism pose significant challenges. The findings highlight the difficulties in ensuring the effective and harmonised implementation of EMFA provisions across the EU, especially in the face of digital platforms' growing dominance over content distribution and public discourse. The article argues that without clear, comprehensive guidance and coordinated efforts to ensure consistent enforcement across Member States, the regulation may fall short in effectively addressing the risks posed to media pluralism, particularly in the rapidly evolving digital environment.

Media pluralism – Media concentration – EMFA – Harmonisation – Enforcement

Dalla retorica alla regolamentazione: EMFA e la concentrazione dei media nell'era digitale

Questo articolo esamina l'evoluzione del discorso politico e delle pratiche relative al pluralismo dei media all'interno dell'Unione europea (Ue) alla luce dello European Media Freedom Act (EMFA), che impone agli Stati membri di valutare l'impatto delle concentrazioni nel mercato dei media sul pluralismo dei media. Attraverso l'analisi di testi legislativi e politici chiave dell'Ue, l'articolo esplora come viene affrontata la concentrazione mediatica, con particolare attenzione a due Stati membri più piccoli (Croazia e Slovenia), dove leggi obsolete e la mancanza di dati per valutare il pluralismo dei media rappresentano sfide significative. I risultati evidenziano le difficoltà nel garantire un'attuazione efficace e armonizzata delle disposizioni dell'EMFA in tutta l'Ue, specialmente di fronte alla crescente posizione dominante delle piattaforme digitali nella distribuzione dei contenuti e nel discorso pubblico. L'articolo sostiene che, senza orientamenti chiari e completi, e sforzi coordinati per garantire un'applicazione uniforme tra gli Stati membri, la regolamentazione potrebbe non riuscire a contrastare efficacemente i rischi per il pluralismo dei media, in particolare in un ambiente digitale in rapida evoluzione.

Pluralismo dei media – Concentrazione dei media – EMFA – Armonizzazione – Applicazione

The Author is Assistant Professor at the Department of Journalism, University of Ljubljana, and a Visiting Fellow at the Robert Schuman Centre, European University Institute, Florence

This paper is part of the monographic section *EMFA under the spotlight: towards a common regulatory framework to foster media pluralism?* edited by Elda Brogi

SUMMARY: 1. Introduction. – 2. Moving target of the EU media policy. – 2.1. Green papers, studies, and expert groups. – 2.2. *From television without frontiers to Audiovisual Media Services Directive*. – 2.3. *European Media Freedom Act*. – 3. Research design and rationale for cases selection. – 4. Case study: Croatia. – 4.1. *Regulatory framework*. – 4.2. *Gaps and reform*. – 5. Case study: Slovenia. – 5.1. *Regulatory framework*. – 5.2. *Gaps and reform*. – 6. Discussion and conclusion: collaboration for harmonisation. – 7. Conclusion.

1. Introduction

Until recently, the European Union (EU) avoided steering regulation of media concentration. There were some attempts, but they failed due to resistance from Member States, which viewed such interference as a threat to their subsidiarity in the media sector. It was believed that this would undermine their sovereignty in pursuing their own social, democratic, and cultural goals within their national media landscapes. The European Commission refrained from advocating for strict regulation, favouring instead the view that regulation should not impede the growth of the European media industry. The goal was to foster the emergence of European champions capable of competing with much larger U.S. companies, which benefit from economies of scale and lighter regulatory frameworks¹. However, this approach backfired, as the integration of the European market largely benefited the American audiovisual industry². At the same time, the findings of the Media Pluralism Monitor³ reveal an overall decline in media pluralism across EU countries. This suggests that insisting on subsidiarity in media-related

matters has not led to enhanced media pluralism at the national level.

With the adoption of the Regulation (EU) 2024/1083⁴, the EU has set a clear mandate for Member States to regulate the impact of media concentration on pluralism. For countries with ineffective or non-existent frameworks to assess media concentration, this presents both an opportunity and a challenge. In the circumstances of already highly concentrated national media markets⁵ the EMFA provides an external push to establish or strengthen regulatory mechanisms, assigning direct or participatory responsibilities to national media regulatory authorities. This opportunity is however shadowed by the fact that new regulations will not have retroactive effects. The problem is further deepened by the growing dominance of global digital players. Acting as gatekeepers, they continue to reshape business models and user behaviour, what makes traditional media concentration concepts and regulatory approaches based on national markets and ownership restrictions increasingly outdated. National regulatory frameworks, although intended to safeguard media pluralism, are limited in their capacity to

1. EUROPEAN COMMISSION 2005.

2. EAO 2023.

3. BLEYER-SIMON et al. 2024.

4. European Parliament and Council of the European Union, [Regulation \(EU\) 2024/1083](#) establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act). Official Journal of the European Union, L 177/1.

5. BLEYER-SIMON et al. 2024; CARLINI 2024.

counter the influence of cross-border platforms that operate beyond national regulatory reach. As Picard and Pickard noted⁶, national policies alone are inadequate in addressing the challenges of a globalized communication environment – an issue that is especially pressing for smaller states, which are even more vulnerable to external pressures and often lack influence in international policymaking⁷. From a broader perspective, recent scholarship emphasizes the need for new regulatory approaches⁸ as regulation risks falling short unless it addresses broader «concentration trends driven by datafication, digitalisation, and platformisation of the media ecosystem»⁹.

Since the success of the EMFA depends on how well the EU Member States can adapt their existing media concentration frameworks and how well national regulators can enforce them in a harmonised way, by taking into account the digital dimensions of the problem, this study examines how media concentration frameworks of EU Member States are adapting following the adoption of the EMFA. Employing document analysis and case studies, the research specifically focuses on small states (i.e., Croatia and Slovenia) as they are facing different challenges in comparison with their larger counterparts with stronger media industries.

The first section offers an overview of the evolution of EU media pluralism and concentration policies, emphasising key legislative milestones and discursive highlights, from the 1992 Green Paper to 2024 EMFA. The second section, where the research design and method are outlined, is followed by the third section, which presents case studies of Croatia and Slovenia – two countries that are comparable in size, market dynamics, and historical background. The fourth section discusses the findings, placing them within the context of

a communication environment increasingly dominated by digital platforms. The article concludes with recommendations to improve enforcement mechanisms through collaborative platforms, ensuring more consistent protection of media pluralism across Member States.

2. Moving target of the EU media policy

Member States, along with supranational entities like the European Commission, the European Parliament, and the Court of Justice of the European Union (CJEU), hold diverse opinions and exert varying levels of influence over EU media policies and regulations – and media pluralism is no exception. Historically, media pluralism has been a highly contentious issue, with numerous unsuccessful regulatory efforts dating back to the 1990s¹⁰. Despite being regarded as one of the foundational principles of liberal democracy¹¹ and widely accepted in contemporary normative media theories, public sphere theories, and media policies, pluralism is rarely examined as a distinct value¹². This opens the door for it to be framed through an economic lens rather than a social or democratic one, allowing it to be used in support of various, often divergent, goals¹³. argues that the concept of media pluralism should not be confined to merely diversity of choices but must also encompass the structural power relations within the media ecosystem, particularly the struggles over the framing of public discussions and decisions shaping media ownership and system architecture. Yet, public discourse often reduces media pluralism to a narrow focus on media ownership. A common theme is the central role of media concentration¹⁴ as high levels of concentration in media ownership are widely believed to restrict the range of voices and viewpoints present in the media.

6. PICARD–PICKARD 2017.

7. BALDACCHINO–WIVEL 2020.

8. BROGI et al. 2023; SEIPP 2023; TRAPPEL–MEIER 2022; BEYER 2018.

9. SEIPP 2023, p. 393.

10. HARCOURT 2005; DOYLE 2007; KARPPINEN 2007.

11. MOUFFE 2000, p. 18.

12. KARPPINEN 2007.

13. KARPPINEN 2013.

14. TRAPPEL 2022; VALCKE 2011.

2.1. Green papers, studies, and expert groups

The 1992 Green Paper on Media Pluralism and Concentration¹⁵ was one of the Commission's earliest responses to the growing concerns about media concentration. It proposed several recommendations aimed at promoting media pluralism and considered legislative options to harmonize media regulations across Member States. However, it encountered significant resistance, particularly surrounding the question of the EU's competence in regulating media matters – traditionally in the domain of Member States. As a result, despite the recognition of the importance of media pluralism, the proposals were shelved.

In 2007, the Commission sought to relaunch the debate on media pluralism through the «three-step approach towards advancing the debate on pluralism within the European Union»¹⁶. This initiative envisaged a working document, independent study, and plan for a policy communication on media pluralism indicators. While the first two were completed successfully, the final step was never pursued. Although this approach demonstrated the EU's ongoing interest in media pluralism, it did not result in the adoption of any regulations, nor did it lead to the issuing of a Commission Communication. The non-binding nature of this initiative underlined the continued reluctance at the time to move toward regulatory harmonisation in such a politically sensitive area.

The High-Level Group on Media Freedom and Pluralism, established in 2011, was another effort to assess and strengthen media freedom and pluralism across Europe. In 2013, the group produced a report with a range of recommendations¹⁷, but their implementation remained largely dependent on the willingness of individual Member States and varied significantly across the EU, demonstrating again the challenges in achiev-

ing a cohesive, EU-wide regulatory framework for media pluralism.

2.2. From television without frontiers to Audiovisual Media Services Directive

In the processes of 1997 and 2007 revisions of Television Without Frontiers Directive (TVWFD¹⁸), discussions around media pluralism played an important role, but they did not lead to any regulatory framework or action. The first revision primarily focused on regulating advertising, while the second one largely aimed at expanding the directive's scope to ensure a level playing field between linear and non-linear audiovisual media services and relaxing the rules on advertising. While media pluralism was part of the debate, especially in the context of safeguarding diverse content in an increasingly liberalised market, the revision did not include binding measures to address media concentration or guarantee media pluralism across Member States. As demonstrated in my previous research¹⁹, among the main topics discussed by stakeholders, media pluralism got the least attention and there was minimal support for including it in the new audiovisual regulatory framework. Contributions primarily came from national institutions, telecom companies, and to a lesser extent, commercial broadcasters, public broadcasters, and civil society. Interestingly, during the revision process that took part between 2003 and 2007, the European Parliament (EP) placed greater emphasis on issues like product placement rather than media pluralism; in EP reports, product placement was referenced over 150 times, whereas media pluralism received significantly fewer mentions²⁰.

This indicates a broader pattern where pluralism is overshadowed by discussions around the market, with a common belief that an open,

15. EUROPEAN COMMISSION 1992.

16. EUROPEAN COMMISSION 2007.

17. VĪĶE-FREIBERGA et al. 2013.

18. European Parliament and Council of the European Union, Directive 97/36/EC amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation, or administrative action in Member States concerning the pursuit of television broadcasting activities (Television Without Frontiers). Official Journal of the European Union, L 202/60.

19. KERŠEVAN SMOKVINA 2014.

20. *Ibidem*.

competitive market ensures media freedom and diversity. This narrative was particularly evident in the speeches of Commissioner Viviane Reding and, to a slightly lesser extent, European Parliament Rapporteur Ruth Hieronymi, where deregulatory efforts were framed as advancing normative ideals such as media freedom and pluralism²¹. Both officials used terms like media freedom, pluralism, and diversity interchangeably²². Diversity typically carried a more tangible meaning, while pluralism was presented as a broader social value²³. Reding, for instance, frequently linked economic liberalisation, such as the deregulation of advertising, with the promotion of media pluralism²⁴. In one typical example, she defended the deregulation of product placement, arguing that «responsible advertising is the economic foundation of a pluralistic media landscape»²⁵. In the final text of the revised TVWF, later consolidated into Directive 2010/13/EU²⁶, media pluralism is referenced six times in the recitals, but the operative text lacks provisions addressing structural factors, such as media concentration.

In the subsequent revision of the Audiovisual Media Services Directive (AVMSD), media pluralism was once again a point of discussion, as the EU sought to address the growing concerns about media concentration and the dominance of global digital platforms. In the final text of the 2018 AVMSD, media pluralism – much like in the 2007 AVMSD – is mentioned six times in the recitals, but the operative provisions (Article 5(2)) are limited to ownership transparency. These provisions allow Member States to introduce laws requiring media service providers to disclose their ownership structures, including beneficial owners, while ensuring the protection of fundamental rights, such as privacy and family life, for those own-

ers. While these media ownership transparency provisions were a step forward, critics argue that the AVMSD fell short of addressing the deeper structural issues related to media ownership and control, particularly as digital platforms continued to grow in influence²⁷. This period illustrates further EU struggle to reconcile liberal market principles with the need for regulation that protect democratic values, such as media pluralism, in an increasingly complex media environment.

2.3. European Media Freedom Act

In 2024, the EMFA finally introduced an EU response to the risks posed by media concentration and its potential impact on media pluralism and editorial independence. The EMFA mandates that Member States establish both substantive and procedural rules to assess media market concentrations that could negatively affect pluralism; these assessments must be conducted in a manner that is transparent, objective, proportionate and non-discriminatory, based on the criteria set in advance (Article 22(1)), ensuring fairness across the EU's diverse media landscapes. When assessing media market concentrations, the following elements must be considered: the impact on media pluralism, including diversity of services and influence on public opinion; safeguards for editorial independence; the economic sustainability of the parties involved; relevant findings from the Commission's Rule of Law report on media pluralism and freedom; and any commitments offered by the parties to safeguard pluralism and editorial independence (Article 22(2)).

The framework is based on cooperation between national regulatory authorities (NRAs) and the newly created European Board for Media Services (Articles 8-13). The NRAs are central to

21. *Ibidem*.

22. *Ibidem*.

23. KARPPINEN 2007.

24. KERŠEVAN SMOKVINA 2014.

25. REDING 2006.

26. European Parliament and Council of the European Union, Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive). Official Journal of the European Union, L 95/1.

27. NENADIĆ–MILOSAVLJEVIĆ 2021.

this process, tasked with conducting (or participating in) assessments of media market concentrations within their jurisdictions (Recital 65). Their independence is essential, as highlighted in the EMFA (Recital 36), which stipulates that NRAs must have the necessary staffing, financial resources, and technical expertise to function effectively (Article 7(3)). NRAs are also empowered to request information from media companies ((Article 7(4)). The Board (together with the Commission) plays an advisory and supervisory role, offering technical expertise, fostering cooperation among NRAs, and facilitating the exchange of information. While its opinions are non-binding, the Board has the authority to review and offer feedback on national actions and rulings that affect media markets and concentration (Article 22 (3-6)).

Although these provisions represent a significant and tangible shift from earlier attempts that were largely rhetorical, the discursive elements remain relevant for further study. The Act mentions terms pluralism and plurality 60 times in total, 48 times in the recitals and 12 times in the operative provisions. Media concentration is referred to 51 times in total, 30 times in the recitals and 21 times in operative provisions. In explaining the motivation behind the proposed model, market dimensions are still at the forefront, but the framing has changed. Instead of the previous avoiding of regulation of media concentration in the name of media pluralism – where excessive regulation was thought to hinder market development, which was considered the best guarantee for preserving pluralism – there is now a noticeable emphasis on the necessity of regulating media concentrations, but with a highlight on ensuring harmonisation across Member States to avoid the existing variance and inconsistencies that could impede the functioning of the internal market and distort competition (e.g., Recital 62). This more nuanced discourse correlates with the evolving complexities in the media ecosystem, where efforts to preserve media pluralism at the national

level intersect with the broader challenges at the supra-national level.

3. Research design and rationale for cases selection

This study investigates and compares the cases of Croatia and Slovenia, which are overlooked in media policy research. In international benchmarks, small countries are either rarely present or sometimes grouped with larger media markets²⁸ that do not share their unique challenges. While Slovenia and Croatia differ in national language – with Slovenian having few speakers outside the country, whereas Croatian is mutually intelligible with the languages of three other former Yugoslav countries, allowing its media industries to extend more easily across national borders – they share several important characteristics beyond their “smallness”. Both were units of the Socialist Federal Republic of Yugoslavia, gaining independence in 1991 and later joining the European Union – Slovenia in 2004 and Croatia in 2013. In the former Yugoslavia, they were the most democratically and economically advanced republics and remain the only two successor states to have joined the EU. In international classifications, both countries appear in the category of small states²⁹. With population of 2.1 million, Slovenia is at the lower end of this category in the European Union, while Croatia’s population is nearly 3.9 million. In economic terms, Slovenia generally performs better. In 2023, Slovenia’s GDP per capita was €30,158³⁰, compared to €19,847 in Croatia³¹. Despite their shared history and strong cultural and business ties, their media landscapes and regulatory environments differ, what makes them a relevant pair for comparative analysis.

The “most similar systems design” model³² allows for a comparative investigation into how their media regulation models are aligning with the EMFA. By focusing on countries with similar characteristics, this model minimizes the risk of overlooking critical details that might otherwise be lost in a comparison of more varied systems,

28. See, e.g., SCHNYDER et al. 2023.

29. TRAPPEL 2014, p. 240.

30. SURS 2024.

31. HNB 2024.

32. SEAWRIGHT–GERRING 2008.

ensuring that key nuances are captured and understood. This study employed document and legal analysis, focusing on the existing laws relevant for media concentration, and the proposals of new or revised laws, in the period from May 2024 to October 2024.

In total, two laws were analysed in Croatia (both in force at the time of writing): the 2004 Media Act (*Zakon o medijima*)³³, which has been amended several times, most recently in 2022, and the 2021 Electronic Media Act (*Zakon o elektroničkim medijima*)³⁴. In Slovenia, the 2001 Mass Media Act (*Zakon o medijih*)³⁵ was examined (having also undergone several amendments since the adoption, with the most significant but targeted one in 2016), together with the draft proposal for a new Mass Media Act of September 2024, which is expected to enter parliamentary procedure by the end of 2024. A key limitation of this research is the time frame, which does not allow for the analysis of the final outcomes of the adaptations of Croatian and Slovenian media legislation to the EMFA. However, this also highlights how lengthy these legislative processes can be. Another limitation is the limited availability of draft legal texts, pointing to issues of low transparency and inclusiveness in both states. The results are presented on a case-by-case basis, beginning with an overview of the legislative and institutional framework governing media concentration. This is followed by a critical analysis of the current framework and the ongoing adaptation to the EMFA.

4. Case study: Croatia

Croatia's media landscape faces significant challenges to media pluralism, as highlighted by the Media Pluralism Monitor (MPM 2024)³⁶. The MPM market plurality indicator shows a high-risk score of 66%, reflecting the dominance of a few key players and increasing consolidation in the

Croatian media market. Media outlets, particularly at the regional and local levels, often depend heavily on public funding, making them vulnerable to both political and commercial pressures, which undermine journalistic autonomy and editorial independence. Although new media legislation is in development, the process is unfolding behind closed doors and without the involvement of key stakeholders, raising criticism of the journalists' association HND and union SNH about the lack of a consultative process³⁷. Additionally, the 2024 Rule of Law Report from the European Commission has raised concerns about media pluralism and the independence of Croatia's media regulatory body³⁸.

4.1. Regulatory framework

Croatia's regulatory framework for media concentration and media pluralism is governed by two key legislative acts: the 2021 Electronic Media Act and the 2004 Media Act. According to the Electronic Media Act, media service providers are required to disclose their ownership structures to the Agency for Electronic Media (AEM) within five days of any change (Article 61). This includes information on both direct and indirect owners, with an emphasis on transparency to prevent hidden ownership or undue control over media companies. Each year, providers must also submit certified documents on acquisition of shares and must publish any changes in the Croatian Official Gazette. According to Article 62, media providers must notify the Competition Authority before proceeding with any merger or acquisition that meets the threshold set by competition law. If requested, the AEM provides expert opinions on such concentrations with a focus on their implications for media pluralism. If the AEM does not respond within 30 days, it is considered that there are no objections. The final decision, however, rests with the Competition Authority, which must assess the

33. *Zakon o medijima* (Media Act). Official Gazette of the Republic of Croatia, No. 59/04, 84/11, 81/13, 114/22,

34. *Zakon o elektroničkim medijima* (Electronic Media Act). Official Gazette of the Republic of Croatia No. 153/09, 84/11, 94/13, 136/13, 152/14, 102/15, 32/19, 70/21.

35. *Zakon o medijih* (Mass Media Act). Official Gazette of the Republic of Slovenia, No. 110/06, 36/08, 77/10, 90/10 – CC, 87/11, 47/12, 47/15, 22/16, 39/16, 45/19 – CC, 67/19 – CC, 82/21.

36. BLEYER-SIMON-BROGI-CARLINI et al. 2024.

37. MFRR 2024.

38. EUROPEAN COMMISSION 2024-B.

economic impact and take into account the potential effects on media pluralism as identified with the AEM (Article 62).

The Media Act contains basic provisions on that in Articles 35 and 36, while also establishing a 40% market threshold for newspapers, beyond which concentrations are not allowed. Other thresholds are defined in the Electronic Media Act. As regards cross-ownership, a media provider with a national broadcasting license is restricted from holding more than 25% of shares in another broadcaster at the same or lower level (Article 64). Moreover, media owners who hold state-level concessions are prohibited from owning more than 10% of a daily newspaper that prints over 3,000 copies. These restrictions are designed to prevent the consolidation of ownership and ensure the diversity of media voices. Another significant provision is Article 65, which establishes that any media provider whose annual revenues account for more than 40% of the total media market revenues in Croatia is considered to have a dominant position. Such providers are prohibited from acquiring additional shares in other media outlets, as this would further concentrate the market and reduce diversity. In terms of enforcement, if a provider fails to comply with the provisions regarding ownership transparency or exceeds the allowed concentration limits, the Council for Electronic Media, which can impose severe sanctions, including revoking broadcasting licenses or other authorizations (Article 63(3)). The Council is a body governing the AEM and is composed of seven members, who are appointed by the Croatian Parliament.

In sum, the main regulatory bodies responsible for regulation of media concentrations include the AEM, the Council for Electronic Media, and the Competition Authority. The latter assesses media concentrations in line with the competition law. The AEM monitors compliance with media ownership regulations, transparency requirements (reporting obligations), and cross-ownership restrictions. The Council holds the sanctioning powers.

4.2. Gaps and reform

Despite the rather comprehensive regulatory framework, there are several gaps as regards its applicability, effectiveness, and purpose. While

the law empowers regulatory bodies to block concentrations that threaten media pluralism, it lacks specific criteria or metrics for assessing these threats. This vagueness can lead to subjective decision-making and inconsistent application of the law. Although public access to data on media ownership has improved since Croatia joined the EU, numerous outlets remain unregistered and there is still insufficient regulation and monitoring to ensure full compliance, making the evaluation of media concentration difficult³⁹. Also, both the Electronic Media Act and the Media Act focus primarily on traditional media (broadcasting and print), with no provisions on digital services. While the law provides for revoking licenses as a penalty for violating media pluralism rules, this severe measure may not always be effectively applied. The lack of graduated sanctions – such as fines or temporary suspensions – limits the regulatory bodies' flexibility in addressing violations of varying severity. The law addresses national media concentrations and lacks sufficient provisions for local media markets, which are more vulnerable to monopolistic practices. The lack of detailed criteria for pluralism, the focus on traditional media, and the limitations in enforcement mechanisms indicate areas that require reform to address contemporary challenges posed by digital platforms and changing media consumption patterns.

At the time of writing, the specifics of the modifications to the existing media frameworks remain unclear. In July 2023, the Ministry of Culture circulated what was widely perceived as a draft proposal for a new Media Act. This proposal faced strong criticism from civil society and public watchdogs. The Croatian Association of Journalists (HND) criticized it for potentially undermining media freedom and journalistic independence, while failing to provide adequate safeguards to protect media pluralism (HND 2023). Additional concerns were raised regarding provisions that would grant publishers excessive influence over editorial content and politicize the appointment process for members of the AEM (ib.). In response, Minister of Culture and Media, Nina Obuljen Koržinek, clarified that the document in question was not a formal draft of the Media Act nor had it been sent into any legislative procedure, but was merely a starting point for dis-

39. VILOVIĆ et al. 2023.

cussions within the working group⁴⁰. By September 2024, the Minister announced plans to form a new working group to draft a comprehensive law that may merge the Media Act and the Electronic Media Act, thus expanding the AEM's mandate to cover print media as well⁴¹. As the new draft is awaited, the HND and the Trade Union of Croatian Journalists (SHN) continue to advocate for a more inclusive and transparent reform process⁴².

5. Case study: Slovenia

Slovenia's media landscape, while featuring a broad range of media, faces significant risks to media pluralism (MPM 2024)⁴³. The market plurality indicator, with a 2024 risk value of 72%, is driven by a strong structural tendency towards media concentration. This has worsened by the dominance of digital platforms, which has not been counterbalanced by innovation in the Slovenia's media. Slovenia has consistently struggled with issues of politicisation in media ownership and the allocation of public resources. Editorial independence is another area of concern, having shifted from medium to high risk in 2024. The Slovenian chapter of the 2024 Rule of Law report⁴⁴ pointed to insufficient safeguards against undue political influence over the appointment process in the Slovenia's national regulatory authority responsible for the media, that is the Agency for Communication Networks and Services (AKOS)).

5.1. Regulatory framework

The Mass Media Act (*Zakon o medijih*) is a key legislative tool that addresses media pluralism and ownership in Slovenia, among other key areas of media regulation. First adopted in 2001, this very comprehensive law has undergone minor amendments. The provisions on media concentration were slightly updated only in 2006. The Ministry of Culture has the primary role in reviewing media mergers and acquisitions that could affect media pluralism. The Act contains several bans and benchmarks aimed at preventing media con-

centration and protecting media pluralism. There are cross-ownership bans between print, radio, and television media, as well as between media and advertising organisations. Entities holding more than 20% of ownership or voting rights in a general daily newspaper cannot also own or establish a radio or television company, and vice versa (Article 56). Article 59 of the law outlines the restriction that a broadcaster may only operate either radio or television services, not both types, unless it secures a license under Article 105. However, as there are no obstacles to obtaining this license, the ban is ineffective in practice, calling into question the necessity of such a provision in the law. There is also a cross-ownership ban aimed at preventing the vertical integration between telecom operators and broadcasters (Article 62 (1)) which is similarly relativised by a provision allowing telecom operators to get the license for broadcasting channels (Article 62 (2)).

According to Article 58, any entity seeking to acquire more than 20% ownership in a media company must first secure approval from the Ministry, which consults with three key institutions. The AKOS provides data on media reach and population coverage, while the Securities Market Agency (ATVP) offers information on connected persons – individuals or entities related through capital, management, or family ties, who could indirectly influence multiple media companies (Article 57). Additionally, the Broadcasting Council, an expert body appointed by the Slovenian Parliament and supported by AKOS administratively, technically, and financially, issues non-binding opinions on the acquisitions. The Ministry assesses whether the acquisition could lead to a dominant position in the advertising market or breach the legal benchmarks regarding coverage. These benchmarks include restrictions on ownership, such as prohibiting any entity from controlling more than 30% of television coverage or 15% of radio coverage. However, these benchmarks specifically refer to analogue broadcasting, making them largely obsolete, particularly since Slovenia

40. VLADA RH 2023.

41. HINA 2024.

42. MFRR 2024.

43. BLEYER-SIMON-BROGI-CARLINI et al. 2024.

44. EUROPEAN COMMISSION 2024-C.

switched to digital television broadcasting in 2010. Additionally, the law imposes a threshold on print media, stipulating that no entity should control more than 40% of daily newspaper circulation in Slovenia. This provision is long overdue, given the significant and steady decline in print circulation as daily newspapers shift toward alternative revenue sources. One Slovenian daily specialising in finance and business went fully digital in 2024, and more publications may follow this trend.

5.2. Gaps and reform

As demonstrated above, the current legislation on media concentrations is outdated to the point of non-applicability. Also, the small and already highly concentrated Slovenian media market is characterised by complex ownership structure with cross-linked ownership chains, where information on the actual media owners is often incomplete or outdated⁴⁵. The Media Registry, managed by the Ministry of Culture, does contain basic information on media outlets and owners holding at least a 5% share, but due to its incompleteness and irregular updates, it fails to provide an accurate picture of ownership structures. Although the transposition of the EU anti money laundering legislation in 2015 has improved ownership transparency in general, there is still a need for a unified and regularly updated database containing all essential information on media ownership. Another significant concern is the role of the Ministry of Culture as the primary decision-maker in assessing and approving media mergers and acquisitions, a unique arrangement that is highly prone to political influence.

In the ongoing media legislation reform, the Government released two versions of a proposed new Mass Media Act – the first in December 2023 and the second in May 2024. Additionally, a leaked version circulated in September 2024. Since this leaked version has been sent for interdepartmental review, and representatives from the Ministry stated at a public event in October 2024 that it is nearing Government approval⁴⁶, this analysis is based on this unofficial (leaked) version. The previously presented public drafts contained different and less elaborated provisions. The proposal grants the responsibility for the assessment of media

concentrations to the AKOS which is the central regulatory authority overseeing telecommunications, digital services, postal and railway services – and electronic media in Slovenia, designated also as Slovenia's Digital Services Coordinator (DSC) under the Digital Services Act (DSA). The proposal envisages that entities intending to acquire control over media outlets or online platforms notify AKOS prior to executing such transactions. The "control" is defined broadly, including mergers, acquisition of ownership or voting rights, and the creation of joint ventures (Article 24). The evaluation process is separate from other competition law reviews, ensuring that media concentration is assessed with a specific focus on its impact on pluralism and the public interest (Article 24(6)). If this version is adopted, AKOS will have 100 working days to evaluate media concentrations and decide whether they pose a threat to media pluralism or editorial independence. Concentrations found to significantly reduce media pluralism will be prohibited (Article 27). AKOS will be also empowered to impose remedial measures, including requiring companies to take specific actions to protect the public interest or editorial independence (Article 38). Additionally, AKOS will be able to fine companies that fail to comply with reporting requirements or engage in unauthorized concentrations (Article 32).

A critical shortcoming in these draft provisions is the lack of benchmarks for assessing media pluralism. Although the draft emphasizes the importance of protecting media diversity and independence, it does not provide any measurable criteria – such as ownership limits, content diversity, or audience reach – by which AKOS could assess risks to pluralism on more factual basis. This absence of specific metrics leaves considerable discretion to AKOS, which could lead to inconsistent enforcement. The draft also envisages that AKOS considers the economic viability of media companies involved in concentrations, and whether there are viable alternatives to ensure their sustainability without compromising media pluralism (Article 27(3)). While this provision recognizes the economic realities facing media outlets, it introduces further complexity into the decision-making process without offering clear guidance on how to balance economic concerns with the need to protect

45. MILOSAVLJEVIĆ–KERŠEVAN 2022.

46. STA 2024.

pluralism. The absence of clear criteria is also in a direct conflict with Article 22(1) of the EMFA which mandates that transparent, objective, proportionate and non-discriminatory criteria are set in advance.

Another issue is the concentration of power within the authority, which, while it has strengthened its expertise and professionalism over three decades of operation, has a weak point in governance. As highlighted by the Rule of Law Report⁴⁷, the Government holds excessive influence in the selection of the Agency's decision-maker, i.e., the Director General. In Slovenia, this is a unique structure, where the Director General acts as an individual authority. The AKOS Council, by contrast, only has general supervisory powers and, apart from approving the work programme, financial plan, annual report, and the agency's statute, is not permitted to intervene in the content or procedures related to the adoption of other general acts and individual decisions, recommendations, or related professional tasks of the agency⁴⁸.

6. Discussion and conclusion: collaboration for harmonisation

Media pluralism though inconsistently defined and rarely problematized⁴⁹, remains a fundamental value in democratic societies and is used as a legitimate basis for various regulatory measures. The EMFA defines it as access to a range of media services reflecting diverse opinions (Recital 64). Member states are expected to autonomously assess the impact of media market concentrations on media pluralism, guided by a yet-to-be-developed set of EU standards with no clear timeline. Now their approaches differ significantly. Some apply only competition assessments, while others involve media regulators in the supervision of market transactions. Under the EMFA, NRAs are also expected to contribute to approvals of media concentrations in other Member States via the Board, particularly where cross-border impacts on the internal media market arise (Articles 13 and 22). However, this poses regulatory challenges due to the diversity of political, cultural, and economic

conditions in Member States, the lack of specialised expertise, and also data.

The case studies of Croatia and Slovenia reveal important insights into these broader challenges of adapting national regulatory frameworks to the EMFA requirements concerning media concentration. While both countries share several similarities, including their size, market characteristics, and historical background, the differences in their approaches to media regulation illustrate how the process of harmonisation, which is essential to the success of EMFA, remains at risk due to variations in legal structures, institutional frameworks, and political influences. In both Croatia and Slovenia, concerns over media pluralism are heightened by the dominance of a few key players, leading to high-risk ratings in the Media Pluralism Monitor (MPM 2024)⁵⁰. Slovenia's outdated 2001 Mass Media Act, although amended several times, has failed to keep pace with the evolution of the media landscape, leaving gaps in the regulation of media ownership. Croatia, on the other hand, is attempting to consolidate its media laws into a single legal framework but has faced criticism from civil society and journalists for lacking transparency and failing to safeguard media freedom and pluralism effectively.

On the top of that, as media landscapes become increasingly shaped by global digital platforms increasingly dominating content distribution, national regulators face the dual task of protecting local media diversity while adhering to EU-wide frameworks that address cross-border digital services. The challenges faced by small countries are – and will be – significantly different from those encountered by larger countries. Smaller countries, with their concentrated markets and often less funds available for the media, may face bigger risks internally, while larger countries with more diverse markets might experience challenges in addressing large-scale and cross-border media corporations. The fragmented regulatory landscape in countries with multiple media regulators, such as Belgium, Germany, and Spain, introduces further complexity in coordinating regulatory actions and

47. EUROPEAN COMMISSION 2024-C.

48. Electronic Communications Code (*Zakon o elektronskih komunikacijah*), Official Gazette of the Republic of Slovenia, No. 130/22 & 18/23 – ZDU-1O, 2022.

49. KARPPINEN 2007; CANTERO GAMITO 2023.

50. BLEYER-SIMON-BROGI-CARLINI et al. 2024.

interpretations of EU-wide rules. Member states, both large and small, may also struggle to maintain independent media oversight and regulatory consistency. As a result, the independence of the Board could be compromised, as it will reflect the independence – or lack thereof – of national regulatory authorities. These risks challenge the EMFA's harmonisation idea and media pluralism impact.

To safeguard a meaningful and effective implementation of the EMFA, which requires transparent and objective criteria, as well as the availability of data, for assessing media concentration across the EU, it would be beneficial for countries – especially smaller or similarly situated ones (like Croatia and Slovenia) – to form collaborative networks mirroring the idea of Article 12 of the EMFA, which envisages a consultation mechanism for the Board allowing it to engage with relevant stakeholders and experts and to conduct consultations. These networks could serve as forums for exchange on best practices and the development of a common framework for media concentration assessment, providing guidance while still allowing for flexibility to accommodate the unique challenges faced by different countries. The participating bodies could work together to define indicators for measuring the impact of media concentrations on media pluralism, produce guidance documents and a voluntary code of conduct for regulators to follow when assessing media concentration.

To implement EMFA effectively and prevent excessive media concentration, it is also essential to establish consistent data collection. Academic institutions could play a significant role here by contributing their research expertise and analytical methods for conducting regular, in-depth and longitudinal analyses of the media market. This could enable the collection of independent data, more

objective evaluations of ownership structures, and the development of new methodological approaches to assess media concentration amidst the digital transformation and evolving media landscape.

7. Conclusion

While the EMFA provides a general foundation and no clear guidance, Member States, particularly smaller ones, where media concentration can significantly impact access to diverse information, should take proactive steps to develop frameworks that respond to their specific needs. A collaborative platform suggested above would not only support the development of a common approach but also ensure that media concentration assessments are performed with clear benchmarks and in line with the goals of the EMFA, thus contributing to more harmonised enforcement across the EU. Institutions such as the Centre for Media Pluralism and Media Freedom (CMPF) which runs the Media Pluralism Monitor and research community from the involved countries could play an important role in these efforts, providing the expertise, analytical tools and data needed to develop objective indicators for media ownership limits, content diversity, and audience reach. These collaborative platforms could also engage in consultations, fostering the exchange of ideas between national and international regulators, experts, and academics, and ensuring that the framework developed is both robust and adaptable, as well as more harmonised as if it is left to each country. This aligns perfectly with Article 12 and Recital 40 of the EMFA, which allow and encourage seeking the guidance from the academia, particularly on issues that extend beyond the audiovisual media sector.

References

- G. BALDACCHINO, A. WIVEL (2020), *Handbook on the Politics of Small States*, Edward Elgar Publishing, 2020
- K. BLEYER-SIMON, E. BROGI, R. CARLINI et al. (2024), *Monitoring media pluralism in the digital era: Application of the media pluralism monitor in the European member states and in candidate countries in 2023*, Centre for Media Pluralism and Media Freedom (CMPF), 2024
- M. CANTERO GAMITO (2023), *The European Media Freedom Act (EMFA) as Meta-Regulation*, in "Computer Law & Security Review", vol. 48, 2023

- R. CARLINI (2024), *Why accurate measuring of media ownership concentration matters*, Centre for Media Pluralism and Media Freedom (CMPF), 4 March 2024
- G. DOYLE (2007), *Undermining Media Diversity: Inaction on Media Concentrations and Pluralism in the EU*, in K. Sarikakis (ed.), "Media and Cultural Policy in the European Union", Brill, 2007
- EUROPEAN AUDIOVISUAL OBSERVATORY (2023), *Top Players in the European Audiovisual Industry – Ownership and Concentration Report*, 2023
- EUROPEAN COMMISSION (2024-A), *2024 Rule of Law Report: Communication and Country Chapters*, 2024
- EUROPEAN COMMISSION (2024-B), *2024 Rule of Law Report – Country Chapter Croatia*, July 2024
- EUROPEAN COMMISSION (2024-C), *2024 Rule of Law Report – Country Chapter Slovenia*, July 2024
- EUROPEAN COMMISSION (2007), *Media Pluralism in the Member States of the European Union*, Commission Staff Working Document, SEC(2007)32, 16 January 2007
- EUROPEAN COMMISSION (2005), *Issues Paper for the Liverpool Audiovisual Conference: Media Pluralism - What should be the European Union's role?*, 2005
- EUROPEAN COMMISSION (1992), *Green Paper on Pluralism and Media Concentration in the Internal Market: an Assessment of the Need for Communitarian Action*, COM(92) 480, 1992
- A. HARCOURT (2006), *The European Union and the Regulation of Media Markets*, Manchester University Press, 2006
- HINA (2024), *Ministrica: U novi zakon možda bude uključen i zakon o elektroničkim medijima* (Minister: The new law may also include the Electronic Media Act), 11 September 2024
- HNB (Croatian National Bank) (2024), *Main macroeconomic indicators*, 17 September 2024
- K. IRION, R. CARLINI, B. KLIMKIEWICZ et al. (2022), *Overview of distribution of advertising revenues and access to and the intensity of use of consumer data*, in European Commission, "Study on media plurality and diversity online", Publications Office of the European Union, 2022
- K. KARPPINEN (2007), *Making a difference to media pluralism: A critique of the pluralistic consensus in European media policy*, in B. Cammaerts, N. Carpentier (eds.), "Reclaiming the media: Communication rights and democratic media roles", Intellect, 2007
- K. KARPPINEN (2013), *Rethinking Media Pluralism*, Fordham University Press, 2013
- T. KERŠEVAN SMOKVINA (2014), *Discourses of EU media policy: The case of the Audiovisual Media Services Directive* (Doctoral dissertation), University of Ljubljana, 2014
- B. KLIMKIEWICZ (2009), *Is the Clash of Rationalities Leading Nowhere? Media Pluralism in European Regulatory Policies*, in A. Czepek, M. Hellwig, E. Nowak (eds.), *Press Freedom and Pluralism in Europe: Concepts and Conditions*, Intellect, 2009
- MFRR (MEDIA FREEDOM RAPID RESPONSE) (2024), *Croatia: Major challenges ahead to improve media freedom*, 2024
- M. MILOSAVLJEVIĆ, T. KERŠEVAN (2022), *Slovenia. News media outlets and owners: Country report 2022*, University of Salzburg, Department of Communication Studies, 2022
- CH. MOUFFE (2000), *The Democratic Paradox*, Verso, 2000
- I. NENADIĆ, M. MILOSAVLJEVIĆ (2021), *Regulating Beyond Media to Protect Media Pluralism: The EU Media Policies as Seen Through the Lens of the Media Pluralism Monitor*, in S.A. Matei, F. Rebillard, F. Rochelandet (eds.), "Digital and Social Media Regulation", Palgrave Macmillan, 2021
- OFCOM (2022), *Media plurality and online news. Discussion document*, 16 November 2022

- C. PAUWELS, K. DONDEERS (2011), *From Television without Frontiers to the Digital Big Bang: The EU's Continuous Efforts to Create a Future-Proof Internal Media Market*, in R. Mansell, M. Raboy (eds.), "The Handbook of Global Media and Communication Policy", Wiley–Blackwell, 2011
- R.G. PICARD, V. PICKARD (2017), *Essential Principles for Contemporary Media and Communications Policymaking*, Reuters Institute for the Study of Journalism, April 2017
- Predlog Zakona o medijih – EVA 2023-3340-0019 (predlog ZMed-1) (Proposal of Mass Media Act), unpublished version of 2 September 2024
- V. REDING (2006), *Europe's free-to-air content and advertising: not one without the other*, World Federation of Advertisers (WFA) Conference, Paris, 15 May 2006
- J. SEAWRIGHT, J. GERRING (2008), *Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options*, in "Political Research Quarterly", vol. 61, 2008, n. 2
- G. SCHNYDER, M. RADL, M. PAJNIK (2024), *Theorizing and mapping media ownership networks in authoritarian-populist contexts: a comparative analysis of Austria, Hungary, Slovenia, and Turkey*, in "Media, Culture & Society", vol. 46, 2024, n. 1
- STA (2024), *STAv živo: Javna razprava o predlogu zakona o medijih v organizaciji Katedre za novinarstvo UL FDV* (Public debate on the draft law on the media, organized by the Department of Journalism of the University of Ljubljana Faculty of Social Sciences), 16 October 2024
- SURS (STATISTICAL OFFICE OF THE REPUBLIC OF SLOVENIA) (2024), *GDP and economic growth*, 13 October 2024
- J. TRAPPEL (2014), *Small States and European Media Policy*, in K. Donders, C. Pauwels, J. Loisen (eds.), "The Palgrave Handbook of European Media Policy", Palgrave Macmillan, 2014
- J. TRAPPEL, W.A. MEIER (2022), *Soaring media ownership concentration: Comparing the effects of digitalisation on media pluralism and diversity*, in J. Trappel, T. Tomaz (eds.), "Success and failure in news media performance: Comparative analysis in the Media for Democracy Monitor 2021", Nordicom, University of Gothenburg, 2022
- P. VALCKE (2011), *Looking for the user in media pluralism regulation: unraveling the traditional diversity chain and recent trends of user empowerment in European media regulation*, in "Journal of information policy", vol. 1, 2011
- VLADA REPUBLIKE HRVATSKE (2023), *Obuljen Koržinek: Ministarstvo nije izradilo nacrt Zakona o medijima, već tekst za raspravu unutar radne skupine* (Obuljen Koržinek: The Ministry did not draft the Media Act, but the text for discussion within the working group), 20 July 2023
- G.E. VIGEVANI, G. MAZZOLENI, M. CECILI, N. CANZIAN (2024), *Monitoraggio del pluralismo dell'informazione nell'era digitale: applicazione del media pluralism monitor negli stati membri dell'Unione europea e nei paesi candidati nel 2023. Rapporto: Italia*, Centre for Media Pluralism and Media Freedom (CMPF), 2024
- V. VÍKE-FREIBERGA, H. DÄUBLER-GMELIN, B. HAMMERSLEY, L.M.P. PESSOA MADURO (2013), *A free and pluralistic media to sustain European democracy*, The Report of the High Level Group on Media Freedom and Pluralism, European Commission, 2013
- G. VILOVIĆ, K. DOŠEN, Z. IVANUŠ et al. (2023), *Croatia. News media outlets and owners: Country report 2023*, University of Salzburg, Department of Communication Studies, 2023



RIVISTA ITALIANA DI
INFORMATICA E DIRITTO

PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0167 • articolo sottoposto a peer review • pubblicato in anteprima il 14 ott. 2024
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale 

ENRICO ALBANESI

Safeguards for the independent functioning of public service media providers. The legal position of domestic legislation that is not in compliance with Article 5 EMFA

The aim of this article is to comment on Article 5 of the European Media Freedom Act (EMFA), about safeguards for the independent functioning of public service media providers, and shaping the legal position of domestic legislation in this field, which will not be in compliance with that article from the date (8 August 2025) when Article 5 EMFA begins to apply.

*EMFA – Public Service Media Provider – Independence – Procedures for the appointment and the dismissal
Funding procedures*

Garanzie per il funzionamento indipendente dei fornitori di media di servizio pubblico. La situazione giuridica della legislazione interna non conforme all'art. 5 EMFA

Scopo del presente articolo è svolgere un commento sull'art. 5 del Regolamento europeo sulla libertà dei media (EMFA) sulle garanzie per il funzionamento indipendente dei fornitori di media di servizio pubblico, delineandosi quindi la situazione giuridica della legislazione interna agli Stati membri che, alla data (8 agosto 2025) di applicazione dell'articolo stesso, non sia conforme all'art. 5 stesso.

*EMFA – Fornitore di media di servizio pubblico – Indipendenza – Procedure di nomina e licenziamento
Procedure di finanziamento*

The Author is Associate Professor of Constitutional Law, Department of Law, University of Genoa

This paper is part of the monographic section *EMFA under the spotlight: towards a common regulatory framework to foster media pluralism?* edited by Elda Brogi

SUMMARY: 1. Introduction. – 2. Comment on Article 5 EMFA: a) the notion of public service media. – 3. (continuation): b) obligations of Member States (also in the light of the Recitals of EMFA and the Recommendations of the Committee of Ministers of the Council of Europe). – 4. The legal position of domestic legislation, that is not in compliance with Article 5 EMFA in this field.

1. Introduction

The European Parliament and the Council of the European Union have recently passed Regulation (EU) 2024/1083 of the European parliament and of the Council of 11 April 2024, establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act).

The aim of this article is commenting Article 5 of the European Media Freedom Act (EMFA), about safeguards for the independent functioning of public service media providers, and shaping the legal position of domestic legislation, that is not in compliance with that article, in this field.

EMFA was published in the *Official Gazette of the European Union* on 17 April 2024. Most of its articles (including Article 5) shall apply from 8 August 2025. However, it is useful to start analysing immediately those provisions under Article 5 EMFA and shape the legal position of domestic legislation in this field in light of that article. In less than one year, Member States shall change

their legislation, if needed, to comply with it. Not surprisingly, this has recently been stressed by the European Commission in its *2024 Rule of Law Report*¹.

The hypothesis that will be demonstrated here is that domestic legislation that is not in compliance with Article 5 EMFA shall be modified as soon as possible, before that article begins to be applicable from 8 August 2025. The legal consequences of such an infringement from that date will also be analysed².

The article will proceed as follows.

First, commenting Article 5 EMFA, it will be demonstrated that the notion of public service media adopted in that article is referred to a subject (and not to activities carried out by subjects) (Section 2). Some reflections will be carried out on the obligations of Member States under Article 5 EMFA (Section 3).

Secondly, some reflections will be carried out on the legal position of domestic legislation, that is not in compliance with that article, in this field,

1. «Given the relevance of [the provisions under Article 5 EMFA] in fostering media freedom and media pluralism, it is important that Member States start putting them into practice as soon as possible, including by addressing the relevant rule of law reports' recommendations, especially in cases where concerns on the matters covered by the EMFA signalled in the rule of law reports have persisted for several years of where deterioration of the situation has been reported». See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *2024 Rule of Law Report. The rule of law situation in the European Union*, COM(2024) 800, p. 25.

2. I have already published an article (in Italian) commenting Article 5 EMFA. See ALBANESI 2024. However, that article specifically focused on the Italian legislation in light of Article 5 EMFA, whereas in the present article I will state that in general domestic legislation of EU Member States, if not in compliance with article 5 EMFA, shall be modified as soon as possible, before that article begins to be applicable from 8 August 2025. I will also analyse the legal consequences of such an infringement from that date.

analysing the legal consequences of such an infringement from the date when Article 5 EMFA begins to be applicable (Section 4).

2. Comment on Article 5 EMFA: a) the notion of public service media

The first issue is to identify the notion of public service media³ adopted by EMFA: is the notion of public service media within EMFA referred to a subject or to activities carried out by subjects⁴?

EMFA adopts a notion of “public service media” that is referred to a subject⁵ (and not to activities carried out by subjects⁶). This conclusion can be drawn from the following arguments.

First, Article 2 EMFA gives the following definition of “public service media provider”: «a media service provider which is entrusted with a public service remit under national law and receives national public funding for the fulfilment of such a remit»⁷. Therefore, such a definition explicitly refers to a subject, the public service media provider.

Secondly, under that definition, that subject is entrusted with a public service remit under national law *and* receives national public funding for the fulfilment of such a remit. It is significant that, when mentioning these two characteristics of that subject, Article 5 EMFA uses the subjunctive conjunctive “and”; whereas the original proposal

of the Regulation used the disjunctive conjunction “or”⁸, as if national public funding was enough to qualify the *activity* of a subject as public service. On the contrary, article 5 EMFA requires a remit to a *subject*.

Thirdly, Article 2 uses the word “remit”, whereas the original version of the Regulation used the word “mission”⁹. The word “remit” is in line with Protocol No. 29 of the *Consolidated version of the Treaty on the functioning of the European Union* and with the public service remit given to a subject¹⁰; whereas the word “mission” reads as much more generic and potentially concerning any activities of a subject.

Finally, it is also important to mention Recital (10) EMFA, under which the notion of public service should not cover «private media undertakings that have agreed to carry out, as a limited part of their activities, *certain specific tasks* of general interest in return for payment» (emphasis added).

At the end of the day, in light of such an interpretation, Article 5 EMFA is applicable to subjects such as *RAI-Radiotelevisione italiana S.p.A.* in Italy, *France Télévisions* in France or *Corporación de Radio y Televisión Española* in Spain.

Under the aforementioned Protocol No. 29, public service remit is conferred, defined and organised by each Member State^{11,12}. However, un-

3. On public service media in a digitalised and international media market, see DONDERS 2021.

4. Actually, such a legal issue is mainly relevant within the Italian legal scholarly debate. In general, on public services, see GALLARATI 2023, p. 250 ff.

5. According to the position of VIGEVANI 2018, p. 241 ff.

6. According to the view of SANDULLI 1978, p. 15.

7. Under Article 2 EMFA, “media service provider” is «a natural or legal person whose professional activity is to provide a media service and who has editorial responsibility for the choice of the content of the media service and determines the manner in which it is organised». “Media service”, under Article 2 EMFA, is «a service as defined by Articles 56 and 57 TFUE, where the principal purpose of the service or a dissociable section thereof consists in providing programmes or press publications, under the editorial responsibility of a media service provider, to the general public».

8. See *Proposal for a regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU COM(2022) 457*, Article 2.

9. *Ibidem*.

10. Protocol No. 29 refers to «broadcasting organizations» that are provided with «the funding of public service» «for the fulfilment of the public service remit».

11. On the various types of European media models, see HALLIN-MANCINI 2004, and TERZIS 2007.

12. «[I]n so far as [...] funding does not affect trading conditions and competition in the Union to an extent which would be contrary to the common interest, while the realisation of the remit of that public service shall be taken into account». However, «public service broadcasting can have its State funding declared to be compliant with

der the Explanatory memorandum of the proposal for the regulation, the initiative takes due account also of Article 4(2) TEU¹³. In other words, the regulation will not interfere with «national identities or regulatory traditions in the media field»¹⁴.

From this perspective, it is interesting to note that national identity does not allow Member States to jeopardise the common values of the European Union under Article 2 TEU¹⁵. If Member States were allowed to undermine such common values, this would mean¹⁶ undermining the substantive constitution of the European Union¹⁷.

Public service media are essential to strengthen freedom of expression and information¹⁸, thus to implement the principle of the rule of law, that is part of the common values of the European Union under Article 2 TEU. Therefore, Member States could not be allowed to jeopardise (in the name of their national identities) such values, when regulating public service media.

Such an issue is not just of a theoretical nature: one should bear in mind that Member States, such as Hungary (that voted against the EMFA proposal within the Council of the European Union¹⁹),

have always used the “national identity” clause as a shield to legitimize their domestic legislation that was not in compliance with the common values under Article 2 TEU²⁰.

This might not be acceptable from the perspective of the European Union, when it comes to public service media.

3. (continuation): b) obligations of Member States (also in the light of the Recitals of EMFA and the Recommendations of the Committee of Ministers of the Council of Europe)

Some specific obligations of Member States are set out by EMFA.

From this perspective, the wording of EMFA is much more precise than the original proposal. In the proposal, «[p]ublic service media providers shall provide in an impartial manner a plurality of information and opinions to their audience», and «[t]he head of management and the members of the governing board of public service media providers shall be appointed through a transparent, open and non-discriminatory procedure and on the basis

the provisions of the Treaty on State aid only inasmuch as the qualitative requirements set out in the public service remit are complied with». See Court of First Instance (Fifth Chamber), Judgment, 16 June 2008, T-422/03, *SIC – Sociedade Independente de Comunicação, SA v. Commission*, paragraph 211.

13. Under Article 4(2) TEU, «[t]he Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State».
14. See *Proposal for a regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act)*, cit., p. 9.
15. Under Article 2 TEU, «[t]he Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail».
16. See VON BOGDANDY–SCHILL 2011, p. 1430 and MANGIAMELI 2012, p. 35.
17. According to the European Court of Justice, the legal structure of the European Union «is based on the fundamental premises that each Member State shares with all the other Member States, and recognises that they share with it, a set of common values on which the EU is founded, as stated in Article 2 TEU». See European Court of Justice (Full Court), *Opinion 2/13*, 18 December 2014, paragraph 168.
18. See Recital (27) EMFA.
19. See Document ST_8553_2024_INIT, Voting result Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act). Adoption of legislative act, 4016th meeting of the Council of the European Union (Agriculture and Fisheries), 26 March 2024, Brussels.
20. See ALBANESI 2021, pp. 115–116.

of transparent, objective, non-discriminatory and proportionate criteria laid down in advance by national law»²¹. EMFA now reads as follows: «*Member States shall ensure that public service media providers are editorially and functionally independent and provide in an impartial manner a plurality of information and opinions to their audience*» (Article 5(1) EMFA); «*Member States shall ensure that the procedures for the appointment and the dismissal of the head of management or the members of the management board of public service media providers aim to guarantee the independence of public service media providers*» (Article 5(2) EMFA) (emphasis added). Therefore, a set of obligations of Member States is now clearly explicit.

Obligations of Member States are those as follows.

(i) Firstly, Member States shall ensure that public service media providers are editorially and functionally independent and provide in an impartial manner a plurality of information and opinions to their audience, in accordance with their public service remit as defined at national level in line with Protocol No. 29 (Article 5(1) EMFA)²².

Editorial and functional independence can be assured by procedures for the appointment and the dismissal of the head of management or the members of the management board of public service media providers that aim to guarantee the independence of public service media providers (as Article 5(2) EMFA reads); by financial resources that safeguard the editorial independence of public service media providers (as Article 5(3) reads); by the monitoring carried out by one or more independent authorities or bodies, or mechanisms free from political influence by government (as Article 5(4) reads).

(ii) Second, Member States shall ensure that the procedures for the appointment and the dismissal of the head of management or the members of the management board of public service media providers aim to guarantee the independence of public service media providers (Article 5(2) EMFA).

In particular, the head of management or the members of the management board of public service media providers shall be appointed on the basis of transparent, open, effective and non-discriminatory procedures and transparent, objective, non-discriminatory and proportionate criteria laid down in advance at national level. The duration of their term of office shall be sufficient for the effective independence of public service media providers.

Moreover, decisions on dismissal of the head of management or the members of the management board of public service media providers before the end of their term of office shall be duly justified, may be taken only exceptionally where they no longer fulfil the conditions required for the performance of their duties according to criteria laid down in advance at national level, shall be subject to prior notification to the persons concerned and shall include the possibility of judicial review.

(iii) Third, Member States shall ensure that funding procedures for public service media providers are based on transparent and objective criteria laid down in advance. Those funding procedures shall guarantee that public service media providers have adequate, sustainable and predictable financial resources corresponding to the fulfilment of and the capacity to develop within their public service remit. Those financial resources shall be such that the editorial independence of public service media providers is safeguarded (art. 5(3) EMFA)²³.

Therefore, principles concerning those procedures under Article 5(3) EMFA are rather generic.

However, some interpretative tips can be taken from Recital (31) EMFA, under which public service media providers benefit from transparent and objective funding procedures which guarantee adequate and stable financial resources for the fulfilment of their public service remit, enable predictability in their planning processes and allow them to develop within their public service remit. Such funding should be preferably decided and appropriated on a multi-year basis, in line with the public service remit of public service media providers,

21. See *Proposal for a regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market*, cit., Article 5.

22. On independence as one of the necessary conditions required to transform a democracy- and citizenship-centric notion of public service media into reality, see DONDERS 2021, pp. 87-89.

23. On adequate funding as one of the necessary conditions required to transform a democracy- and citizenship-centric notion of Public Service Media into reality, see DONDERS 2021, pp. 89-92.

in order to avoid the risk of undue influence from yearly budget negotiations²⁴.

‘Donations’ by the Executive to the public service media providers, as those done within the yearly Budget Act, do not comply with such requirements because they rely on yearly political negotiations on the budget and undermine the independence of the public service media provider: public service media providers cannot rely on funding that does not allow them to plan their activities on a multi-year basis.

(iv) Finally, Member States shall designate one or more independent authorities or bodies, or put in place mechanisms free from political influence by government, to monitor the application of paragraph 1, 2 and 3 (Article 5(4) EMFA).

At the end of the day, the whole principles set out under Art. 5(1), (2), (3) and (4) are rather generic.

However, once again, some interpretative tips can be taken from Recital (31) EMFA, under which Member States shall put in place effective legal safeguards for the independent functioning of public service media providers, «building on the international standards developed by the Council of Europe in that regard»²⁵. From this perspective, it is important to note the relevance of the guidelines that can be found within the 1996 and 2012 Recommendations of the Committee of Ministers of the Council of Europe²⁶.

For example, when it comes to the procedures for the appointment and dismissal of the head of management or the members of the management board of public service media providers, the Committee of Ministers recommends that: there is clear criteria for the appointments that are limited, and directly related, to the role and remit of the public service media; the appointments are not used to exert political or other influence over the operation of the public service media; the appointments are made for a specified term that can only be shortened in limited and legally defined circumstances – which should not include differences

over editorial positions or decisions. As for the funding, the recommendations are as follows: the public service media are consulted over the level of funding required to meet their mission and purposes, and their views are taken into account when setting the level of funding; the funding provided is adequate to meet the agreed role and remit of the public service media, including offering sufficient security for the future as to allow reasonable future planning; the process for deciding the level of funding should not be able to interfere with the public service media’s editorial autonomy.

It is also important to mention the case-law of the European Court of Human Rights (ECtHR). In 2009, the ECtHR stated that the standards relating to public service broadcasting which have been agreed by the Contracting States through the Committee of Ministers of the Council of Europe provide guidance as to the approach which should be taken to interpreting Article 10 of the European Convention on Human Rights (ECHR) on freedom of expression in this field²⁷.

At the end of the day, the aforementioned Recitals of the EMFA and the Recommendations of the Committee of Ministers of the Council of Europe, can provide a guidance to Member States in setting out procedures and criteria required by Article 5 EMFA.

4. The legal position of domestic legislation, that is not in compliance with Article 5 EMFA in this field

As already mentioned, EMFA, published in the *Official Gazette of the European Union* on 17 April 2024, shall apply from 8 August 2025, as for most of its articles, included Article 5.

It is now time to focus on the legal position of domestic legislation that will not be in compliance to Article 5 EMFA and the legal consequences of such an infringement from that date.

(i) Domestic legislation that will not be in compliance with Article 5 EMFA will constitute an in-

24. See Recital (31) EMFA.

25. *Ibidem*.

26. See Council of Europe, Committee of Ministers, *Recommendation No. R (96) 10 on the guarantee of the independence of public service broadcasting*, and Council of Europe, Committee of Ministers, *Recommendation CM/Rec (2012) 1 on public service media governance*.

27. See European Court on Human Rights (Fourth Section), *Manole and others v. Moldova*, 17 September 2009, application No. 13936/02, paragraph 107.

fringement of EU law from 8 August 2025. Therefore, Member States, with such domestic legislation, could be subject to infringement proceedings initiated by the European Commission. In parallel, any domestic court could ask the European Court of Justice to issue a preliminary ruling, in order to have Article 5 EMFA interpreted in the sense that it does not permit such domestic legislation.

From the perspective of domestic legislation, domestic Courts are not allowed to disapply domestic legislation that is not in compliance with Article 5 EMFA. Although EMFA is a Regulation (thus, it is directly applicable in Member States under Article 288 TFEU), Article 5 EMFA does not contain provisions that can be immediately applied: therefore, it is not possible to disapply any domestic provision that is not in compliance with it. As already mentioned in the previous Sections, under Article 5 EMFA Member States shall pass some domestic legislation to follow up the obligations under Article 5 EMFA, such as establishing some procedures to appoint/dismiss the head of management or the members of the management board of public service media providers, in order to guarantee the independence of public service media providers; and some funding procedures for public service media providers based on transparent and objective criteria laid down in advance.

However, a case of constitutionality can be brought before domestic constitutional courts, when under the domestic system of constitutional review, such a kind of antinomy between non-immediately-applicable EU provisions and domestic legislation is the task of constitutional courts²⁸.

(ii) One might also wonder what the status of the head of management or the members of the management board, that were elected after 8 August 2025 on the basis of domestic legislation that is not in compliance with Article 5 EMFA, would be.

From the perspective of EU law, such an action of a Member State would constitute an infringement to EU law, as well. Administrative praxis (that implements EU law) that is not in compliance to EU law can also pose an infringement²⁹. However, such a praxis shall be «to some degree, of a consistent and general nature»³⁰.

From the perspective of domestic legislation, should the constitutional court declare void domestic legislation that is not in compliance with Article 5 EMFA, the appointment of the head of management or the members of the management board elected under such a legislation, would not be legitimate as well.

(iii) Some final reflections should be made from a different perspective, that is of the European Court of Human Rights.

One should bear in mind the aforementioned guidelines that can be found within the 1996 and 2012 Recommendations of the Committee of Ministers of the Council of Europe. Should domestic legislation violate those guidelines, a case-law could be brought before the European Court of Human Rights, in light of violation of Article 10 ECHR on freedom of expression in this field. As mentioned, that was the tool chosen by some journalists of the public service media provider that led the ECtHR to declare a violation of Article 10 ECHR by Moldova in 2009³¹.

References

- E. ALBANESI (2024), *I media di servizio pubblico ex art. 5 del regolamento europeo sulla libertà dei media* (European Media Freedom Act). *Commento dell'articolo ed analisi critica della legislazione italiana in materia*, in "Astrid Rassegna", 2024, n. 6
- E. ALBANESI (2021), *National identity (under Art. 4(2) TEU) and constitutional identity (as counter-limits) are not the same*, in M. Belov (ed.), "Peace, Discontent and Constitutional Law. Challenges to Constitutional Order and Democracy", Routledge, 2021

28. This is the case of Italy. See Constitutional Court, Judgement 8 June 1984, n. 170, section 5 *Considerato in diritto*.

29. See PRETE 2017, p. 57-58.

30. *Ivi*, p. 58.

31. See European Court on Human Rights (Fourth Section), *Manole and others v. Moldova*, 17 September 2009, cit.

- K. DONDERS (2021), *Public Service Media in Europe. Law, Theory and Practice*, Routledge, 2021
- F. GALLARATI (2023), *La dimensione costituzionale del servizio pubblico. Un itinerario comparato*, Editoriale Scientifica, 2023
- D.C. HALLIN–P. MANCINI (2004), *Comparing Media Systems. Three Models of Media and Politics*, Cambridge University Press, 2004
- S. MANGIAMELI (2012), *The Union's Homogeneity and Its Common Values in the Treaty on European Union*, in H.J. Blanke–S. Mangiameli (eds.), “The European Union after Lisbon. Constitutional Basis, Economic Order and External Action”, Springer, 2012
- L. PRETE (2017), *Infringement Proceedings in EU Law*, Kluwert Law International, 2017
- A.M. SANDULLI (1978), *La libertà d'informazione*, Giuffrè, 1978
- G. TERZIS (ed.) (2007), *European Media Governance. National and Regional Dimension*, Intellect, 2007
- G.E. VIGEVANI (2018), *I media di servizio pubblico nell'età della rete. Verso un nuovo fondamento costituzionale, tra autonomia e pluralismo*, Giappichelli, 2018
- A. VON BOGDANDY–S. SCHILL (2011), *Overcoming Absolute Primacy: Respect for National Identity under the Lisbon Treaty*, in “Common Market Law Review”, vol. 48, 2011



MATTEO MONTI

The missing piece in the DSA puzzle? Article 18 of the EMFA and the media privilege

This article examines the provisions of Articles 18 and 19 of the European Media Freedom Act (EMFA) in relation to the digital governance framework established by the Digital Services Act (DSA), with a particular focus on the media privilege codified in Article 18 of the EMFA. Section 2 analyses the media privilege of Articles 18 and 19 of the EMFA from three perspectives: the requirements for obtaining this privilege and the media entities eligible for it; the functioning of the privilege and its intersections with the DSA provisions; and the transparency in its application, including the role of the Board under Article 19 of the EMFA. Section 3 explores the regulatory framework governing the media privilege in Article 18 of the EMFA and addresses criticisms of this online media privilege. More specifically, it focuses on two main criticisms: the risk of granting this privilege to agents of disinformation and the “constitutional” legitimacy of the privilege. The final remarks summarise the main considerations of the different sections and offer concluding observations.

Media privilege – EMFA – Freedom of expression – Media Freedom – DSA – Content moderation

Il pezzo mancante nel mosaico del DSA? L'articolo 18 dell'EMFA e il privilegio dei media

L'articolo esamina le disposizioni degli articoli 18 e 19 dell'European Media Freedom Act (EMFA) in relazione al quadro della governance digitale definito dal Digital Services Act (DSA), con particolare attenzione al privilegio mediale codificato nell'articolo 18 EMFA. La sezione 2 analizza il privilegio dei media di cui agli articoli 18 e 19 EMFA da tre punti di vista: i requisiti per ottenere questo privilegio e i soggetti mediali che possono beneficiarne; il funzionamento del suddetto privilegio e le sue intersezioni con il DSA; i meccanismi di trasparenza e il ruolo del Comitato ex articolo 19 EMFA. La sezione 3 esplora il quadro costituzionale che sottende il privilegio per i media di cui all'articolo 18 EMFA e affronta le critiche a questo privilegio mediale. In particolare, la sezione si sofferma su due critiche: il rischio di accordare questo privilegio ad agenti attivi nelle campagne di disinformazione e la legittimità “costituzionale” di tale privilegio. Le osservazioni finali riassumono le principali riflessioni e offrono alcune osservazioni conclusive.

Privilegio mediale – EMFA – Libertà d'espressione – Libertà d'informazione – DSA – Moderazione dei contenuti

The Author is Visiting Fellow, Max Weber Programme for Postdoctoral Studies, European University Institute, Florence

This paper is part of the monographic section *EMFA under the spotlight: towards a common regulatory framework to foster media pluralism?* edited by Elda Brogi

SUMMARY: 1. Introduction. – 2. The Regulation of Article 18 of the EMFA: the changes from Article 17 of the previous Proposal for a Regulation and the interactions with the DSA. – 2.1. *Which media actors are entitled to the media privilege of Article 18? An analysis of Sections 1, 2, and 3 of Article 18 of the EMFA.* – 2.2. *The media privilege(s) in the platformised public sphere: intersections between the DSA and the EMFA.* – 2.3. *Transparency mechanisms in the application of the media privilege(s) and the Board: section 8 of Article 18 and Article 19 of the EMFA.* – 3. The innovations of Article 18 of the EMFA against the previous regulatory tools and criticism of the media privilege provision. – 4. Final remarks.

1. Introduction

This article examines the provisions of Articles 18 and 19 of the European Media Freedom Act (EMFA)¹ in relation to the digital governance framework established by the Digital Services Act (DSA)², with a particular focus on the media privilege codified in Article 18 of the EMFA. The DSA's regulation of online public discourse is a puzzle composed of different, complementary, regulatory tools, from codes of conduct to the GDPR³. The final piece of this puzzle appears to be Article 18 of the EMFA. Article 18 formalises the role of traditional media within the EU's digital governance structure, specifically in the regulation of public discourse on social media platforms and digital platforms. This Article can be seen as the missing piece in the DSA's approach to regulating online public discourse; it complements the procedur-

alising of content moderation⁴ by introducing a specific regulatory regime for media. The media privilege outlined in Article 18 of the EMFA builds on the debate initiated by the DSA regarding the media's role in the platformised public sphere (see Section 3) and seeks to restore a space for professional journalism in the digital environment. The European Commission's Communication *Tackling Online Disinformation: A European Approach* had already recognised the "need to rebalance the relation between media and online platforms"⁵; however, the DSA did not establish a specific regime for this purpose. The EMFA, on the other hand, establishes such a regime for media within the platformised public sphere: under Article 18 of the EMFA, compliant media have the right to receive the reasons for content removal before it occurs and may respond within 24 hours; they also have the right to have their complaints reviewed

1. Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act).
2. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
4. ORTOLANI 2022.
5. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions *Tackling online disinformation: a European Approach*, COM/2018/236, p. 14.

with priority; and they can initiate direct dialogues with platforms if they believe they are being unfairly censored.

The rise of social media and the increasing reliance of EU citizens on digital platforms for news consumption have led to a situation where «professional journalism and traditional mass media, which largely organised publics, are increasingly bypassed as gatekeepers of public communication flows with the help of digital and social media»⁶. While the democratisation of communication has enhanced pluralism, it has also amplified the spread of misinformation and disinformation, leading also to growing distrust in epistemic communities (including professional journalists)⁷. The EMFA, in alignment with other EU instruments such as the Code of Practice on Disinformation⁸ (see Section 3), seeks to address this challenge by granting traditional media certain privileges on Very Large Online Platforms (VLOPs). In this context, “traditional media” refers to media entities subject to regulatory or co-regulatory mechanisms within the EU Member States.

This article focuses on the specific media privilege⁹ provided by the EMFA on VLOPs. This privilege aims to safeguard the presence of news content produced by professional journalism on VLOPs and identifies the specific constitutional approach of the European Union. Section 2 analyses the provisions of Articles 18 and 19 of the EMFA in comparison with the previous version of the *Proposal for a Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU* (hereinafter referred to as the “Proposal for a Regulation”)¹⁰. Section 2 covers three perspectives: the media entities eligible for digital privileges; the nature of this privilege and intersections between the DSA and the EMFA; the transparency in applying these privileges, and the role of the Board

as outlined in Article 19 of the EMFA. Section 3 explores the digital governance context in which these EMFA provisions operate and discusses potential critical issues. The paper concludes with some summary remarks and reflections.

2. The Regulation of Article 18 of the EMFA: the changes from Article 17 of the previous Proposal for a Regulation and the interactions with the DSA

This Section examines the intersections between the EMFA and the DSA, focusing on the provisions of Articles 18 and 19 of the EMFA as they have evolved from the earlier Proposal for a Regulation. The analysis explores these Articles from three key perspectives: the identification of media entities entitled to the privilege, the nature of the media privilege itself and its interactions with the DSA, and the transparency requirements alongside the role of the Board as outlined in Article 19 of the EMFA.

In conducting this analysis, particular attention is also given to the amendments made to the EMFA provisions compared to the Proposal for a Regulation. These changes are crucial for understanding how some of the initial criticisms of this new media privilege system, designed to “protect” traditional media on VLOPs, have been addressed by the updated provisions of the EMFA.

2.1. Which media actors are entitled to the media privilege of Article 18? An analysis of Sections 1, 2, and 3 of Article 18 of the EMFA

This Subsection addresses the question of which media entities are entitled to the digital privilege under the EMFA when operating on VLOPs. Article 18(1)(a-b) of the EMFA mandates that VLOPs establish a mechanism allowing media to self-declare as media service providers in compliance with Article 6(1) EMFA (transparency

6. SEELIGER–SEVIGNANI 2022, p. 10.

7. NICHOLS 2017.

8. EUROPEAN COMMISSION 2022.

9. CAPPELLO 2017.

10. Proposal for a Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU, COM/2022/457.

obligations)¹¹. More specifically, these media entities also have to assert their editorial independence from Member States, political parties, and third countries (or entities controlled or financed by third countries) (Art. 18, 1, c). To benefit from this media privilege, media actors have to self-declare their editorial independence and confirm that they are subject to the «regulatory requirements for the exercise of editorial responsibility» in at least one EU Member State (Art. 18, 1, d). Thus, they have to declare their commitment to editorial standards recognised within the EU and, additionally, to be subject to the oversight of the «competent national regulatory authority or body or that they adhere to a co-regulatory or self-regulatory mechanism governing editorial standards» (Art. 18, 1, d). Furthermore, Article 18(1) EMFA requires that media entities seeking this protection have to declare that they do not provide content produced by artificial intelligence (AI) without human supervision (Art. 18, 1, e). Finally, these entities have to provide both a quick contact method (Art. 18, 1, f) and the contact details of «relevant national regulatory authorities or bodies or representatives of the co-regulatory or self-regulatory mechanisms referred to in point (d)» (Art. 18, 1, g).

Compared to Article 17 of the previous Proposal for a Regulation, which required media entities to declare their status as media, their editorial independence from the Member States and third countries, and their subjection to «regulatory

requirements for the exercise of editorial responsibility» (Art. 17 of the Proposal for a Regulation), Article 18 of the EMFA introduces additional elements to ensure that the media privilege is granted to entities engaged in journalism practices governed by ethical and professional standards. Notably, the requirement for independence is expanded to include independence from entities controlled or financed by third countries and political parties. The transparency obligations are also reinforced by reference to Article 6 of the EMFA, and the enactment of the AI Act brings automated journalism practices under scrutiny, requiring human oversight of AI-generated content.

The strengthened editorial independence requirements raise questions about their practical application, particularly concerning public financing of news media or their interaction with those news media in which some shares are owned by political parties¹². However, those enhanced requirements clearly address some concerns raised by academics and journalists regarding the risk of extending the media privilege to disinformation agents. Not by chance, the provision is designed to exclude media entities indirectly controlled or financed by third countries from the protection granted by Article 18 of the EMFA¹³.

As an additional safeguard to ensure that the privilege is reserved for media entities committed to professional and ethical journalism, Article 18(1) of the EMFA stipulates that if VLOPs have doubts

11. «Duties of media service providers. 1. Media service providers shall make easily and directly accessible to the recipients of their services up-to-date information on: (a) their legal name or names and contact details; (b) the name or names of their direct or indirect owner or owners with shareholdings enabling them to exercise influence on the operation and strategic decision making, including direct or indirect ownership by a state or by a public authority or entity; (c) the name or names of their beneficial owner or owners as defined in Article 3, point (6), of Directive (EU) 2015/849; (d) the total annual amount of public funds for state advertising allocated to them and the total annual amount of advertising revenues received from third-country public authorities or entities». Article 6, Regulation (EU) 2024/1083.

12. VAN DRUNEN et al. 2023, p. 152.

13. The EU had already committed to combating disinformation from media linked to authoritarian governments of third countries, such as Russian media, in the context of the invasion of Ukraine (Regulation (EU) 2022/350). The EU Tribunal has also upheld this by focusing on the disinformation created by these actors: «As regards the objectives pursued by the Council, recitals 4 to 10 of the contested acts refer to the need to protect the Union and its Member States against disinformation and destabilisation campaigns conducted by the media outlets under the control of the leadership of the Russian Federation which threatened the Union's public order and security, in a context marked by military aggression against Ukraine. Those objectives thus relate to public interests which aim to protect European society and form part of an overall strategy (see paragraphs 11, 12, 14, 17 and 19 above), which is designed to put an end, as quickly as possible, to the aggression suffered by Ukraine». Judgment of the General Court (Grand Chamber) of 27 July 2022, *RT France v Conseil*, T-125/22, par. 55.

about whether a media entity meets «regulatory requirements for the exercise of editorial responsibility» or is subject to oversighting by a regulatory body, «the provider of a very large online platform shall seek confirmation on the matter from the relevant national regulatory authority or body or the relevant co-regulatory or self-regulatory mechanism». The inclusion of contact information for these national regulatory authorities or bodies, as provided by the self-declaring media, is intended to facilitate this verification process. This element clearly places some responsibilities on VLOPs to verify the legitimacy of media entities seeking to use the mechanism of Article 18 of the EMFA.

The intention to support media engaged in professional and ethical journalism is also evident in the restriction of the privilege to entities that employ human oversight in automated journalism. This requirement aims to promote the responsible use of AI in news dissemination and to prevent the spread of unreliable content generated by AI¹⁴. While some critics have expressed concerns that this could create a “chilling effect” by restricting unchecked AI use¹⁵, it is important to note that the privilege afforded to the press in Europe carries with it responsibilities and duties to ensure the accuracy of the content it produces. Therefore, it seems appropriate that AI-generated content should also adhere to the standards of factual correctness that underpin journalism’s role in a democratic society.

Finally, in contrast to Article 17 of the Proposal for a Regulation, Article 18(2) of the EMFA requires that, aside from the legal name and quick contact information of the media, all other elements of the self-declaration have to be made public and accessible. This enhancement of transparency mechanisms allows for the development of accountability measures involving civil society, enabling researchers and journalists to scrutinise the actual characteristics of media entities granted the media privilege under Article 18 of the EMFA and to evaluate the concrete functioning of this provision.

From a “technical” perspective, Article 18(3) of the EMFA establishes a “structure” for the acceptance of the declaration, including the provision of an email address by VLOPs to facilitate the com-

munications between media service providers and VLOPs, thereby ensuring the smooth operation of the media privilege mechanism.

In summary, Sections 1, 2, and 3 of Article 18 of the EMFA outline the requirements for self-declaration as a media entity, including certain controls and specific transparency obligations, and establish the procedure for submitting the application. These provisions collectively define which entities are entitled to the media privilege on VLOPs. But what exactly does this media privilege entail?

2.2. The media privilege(s) in the platformised public sphere: intersections between the DSA and the EMFA

As mentioned in the Introduction, the media privilege under Articles 18 and 19 of the EMFA operates as an exception to the general content moderation system of VLOPs. To fully grasp the scope and structure of this privilege for media entities that have submitted a declaration under Article 18(1) of the EMFA, it is essential to outline in brief the content moderation processes structured by the DSA. The DSA primarily governs the removal of content on VLOPs through two key provisions. Article 9 of the DSA mandates the removal of illegal content at the injunction of judicial or administrative authorities, while Article 14 of the DSA allows platforms to remove content considered incompatible with their terms of service. Where content removal is not requested by public authorities, such as when content is removed following the notice of a user or is taken down by platforms on their own initiative under Article 14 of the DSA, platforms are obligated to provide the affected user with the reasons for such “sanction” *after* the actual removal (Article 17 of the DSA, *Statement of reasons*). The DSA also provides for an “appeal” system for users to challenge these content moderation decisions under Article 20 of the DSA (*Internal complaint-handling system*), along with the possibility of recourse to out-of-court dispute resolution mechanisms (Article 21 of the DSA, *Out-of-court dispute settlement*). The media privilege, or rather the online media privileges outlined in Article 18 of the EMFA, operates within this scenario of content removal under Article 14 of the DSA.

14. MONTI 2018, p. 139.

15. VAN DRUNEN et al. 2023.

The first media privilege provided for by Article 18 of the EMFA requires VLOPs to notify media recognised by Art. 18(1) of the impending suspension or removal of content *before* taking action and to provide an opportunity for a quick response to prevent the content's removal or the suspension of the account. According to Article 18(4) of the EMFA, if a VLOP intends to remove content, reduce its visibility, or suspend the account of a media entity that has made a declaration under Article 18(1) of the EMFA, the platform has to communicate the reasons for this action, pursuant to Article 17 of the DSA, «prior to such a decision to suspend or restrict visibility taking effect» (Art. 18(4)(a)). Unlike the treatment reserved to “ordinary” users, traditional media entities are given a 24-hour window to respond and contest the removal or visibility restriction (Art. 18(4)(b)). In crisis situations, as defined under Article 36 of the DSA, a shorter response time may be applied¹⁶. This privilege for media is designed to protect the presence of media content on digital platforms, safeguarding it against unjustified removals that could impact public discourse and the right of EU citizens to be informed. In this way, the presence of content from traditional media is safeguarded by guaranteeing a right of reply before any removal of the content. The procedure provided for by the EMFA ensures the protection of content that may be of public interest on VLOPs, helping to prevent inappropriate removals. This provision establishes a clear exception to Article 17 of the DSA by mandating that platforms notify traditional media entities of the reasons for content removal *before* taking action, along with a quick redress mechanism, thereby ensuring the protection of traditional media content in the platformised public sphere. If a VLOP rejects the media entity's quick “appeal” and proceeds with the removal, the platform has to communicate this decision promptly to the media affected by it. An exception to this privilege applies when the removal complies with platforms' «obligations pursuant to Articles 28, 34 and 35 of Regulation (EU) 2022/2065 and Article 28b of Directive 2010/13/EU or with their obligations relating to illegal content pursuant to Union law» (Art. 18(4)). This exception ensures that, for instance, in the area of systemic risk management –

including disinformation – the “pre-removal notice privilege” and “quick appeal mechanism” do not apply. Ultimately, Article 18(4) of the EMFA refines the provisions initially proposed in Article 17 of the Proposal for a Regulation, introducing a 24-hour response window for media and clearly defining the exceptions to the application of the privilege.

The second media privilege pertains to an expedited handling of complaints of media recognised under Art. 18(1) of the EMFA against content moderation decisions made by VLOPs under Article 14 of the DSA. Article 18(5) of the EMFA stipulates that complaints by media entities regarding content removal have to be processed «with priority and without undue delay». Additionally, Article 18(5) of the EMFA states that «media service provider may be represented by a body in the internal complaint-handling process». This privilege aligns with the first one by ensuring that media content receives greater protection than that of “ordinary” users, emphasising the special status of media content in the online public discourse. On the one hand, errors in the removal of media content can be corrected more quickly than those affecting “ordinary” users, as media content is considered more relevant to the public interest. On the other hand, representatives of the media's voices and petitions can be included in the evaluation processes of content moderation decisions. Thus, this privilege prioritises “appeals” by traditional media, creating an exception to Article 20 of the DSA, which concerns the internal “appeal” mechanism against content moderation decisions by digital platforms. Compared to the original text in Article 17 of the Proposal for a Regulation, Article 18(5) of the EMFA introduces the possibility of traditional media being represented in the Internal complaint-handling system, creating another exception to Article 20 of the DSA. This addition enhances the privilege by allowing traditional media representatives to participate in content moderation review processes, thereby assisting in the decisions made by the platforms. By prioritising media complaints and allowing for representation in the complaint process, this provision further institutionalises the role of traditional media in the online public sphere.

16. In anyway, the shorter timeframe has to allow «the media service provider sufficient time to reply in a meaningful manner», Art. 18(4)(b).

The third media privilege for media recognised under Article 18(1) relates to the establishment of a direct dialogue channel between platforms and media entities that have obtained recognition under Article 18(1) of the EMFA. Article 18(6) of the EMFA provides that if a media entity believes a VLOP has unjustifiably and repeatedly restricted or suspended its content, it can initiate a «meaningful and effective dialogue with the media service provider, at its request, in good faith with a view to finding an amicable solution, within a reasonable timeframe, for terminating unjustified restrictions or suspensions and avoiding them in the future». This provision diverges from the standard “appeal” mechanism under the DSA, offering a strengthened dialogue mechanism specifically designed to protect media entities. Therefore, Article 18(6) establishes a direct dialogue channel that departs from the appeal mechanism of the DSA, as well as from Article 23 of the DSA (*Measures and protection against misuse*), by creating a strengthened dialogue mechanism specifically designed to protect certain platform users, namely, media subjects. Instead of facing suspensions or sanctions for repeated violations under Article 23 of the DSA, media subjects can initiate a mechanism addressing the “misuse” of terms of service by platforms. In this process, media entities can also involve the Board established by the EMFA (see next Subsection) and the European Commission, further reinforcing the protection afforded to traditional media. Media can communicate the outcome of such a dialogue to the Board and the Commission. Additionally, the Board, at the request of the media involved in the dialogue, can issue an opinion and propose «recommended actions for the provider» (Art. 18(6)). The Board may, in turn, inform the Commission of this opinion. Compared to Article 17 of the previous Proposal for a Regulation, the role of the Board has been strengthened, and the involvement of the Commission has been included, further reinforcing the role of third-party actors as guarantors or advisors in this process for the protection of traditional media subjects. Once again, the purpose of this provision is to ensure the continued presence of traditional media content in the online public discourse. Should the dialogue fail to yield a solution, or if the media entity’s declaration under Article 18(1) is rejected, recourse to the mechanisms under Article 12 of Regulation

(EU) 2019/1150 and Article 21 of Regulation (EU) 2022/20 is available, with the possibility of notifying the Board of the outcome. In this case, too, the Board can be notified of the result achieved. This additional privilege aligns with the previous ones, empowering traditional media in the platformised public sphere against the censorship powers of digital platforms. It is clear that Article 18 of the EMFA protects a specific function of traditional media – the provision of news to the general public – and thus recognises their essential role in the functioning of democracies and public discourse.

In sum, this array of privileges aims to ensure that traditional media can effectively contribute to online public discourse and maintain their crucial role in informing citizens. These privileges are balanced by “accountability” mechanisms, including transparency requirements and the oversight role of the Board under Article 19 of the EMFA.

2.3. Transparency mechanisms in the application of the media privilege(s) and the Board: section 8 of Article 18 and Article 19 of the EMFA

Transparency mechanisms are regulated primarily by the final Section of Article 18 and by Article 19 of the EMFA. Article 18(8) of the EMFA introduces several transparency requirements concerning the number of removals of media content (18.8.a), the reasons for these removals (18.8.b), the number of “amicable” dialogues initiated (18.8.c), the cases in which Article 18(1) of the EMFA declaration was rejected (18.8.d), and the instances where it was invalidated (18.8.e). This provision expands the disclosure requirements compared to Article 17 of the Proposal for a Regulation, which only mandated reporting the number of restrictions and the reasons for them. All these data have to be made publicly available on an annual basis (Article 18.8). This ensures that civil society, journalists, researchers, and others can evaluate the effectiveness of the media privilege of Article 18 of the EMFA. By increasing transparency on the management of content moderation by digital platforms regarding traditional media products and by clarifying which entities have been granted the media privilege, this provision is crucial for evaluating public policy in this field.

Article 19 of the EMFA, on the other hand, establishes an additional form of scrutiny over VLOPs’

content moderation of media products: the presence of the Board. The Board is tasked with organising structured dialogues between platforms, media, and civil society representatives to develop best practices under Article 18 of the EMFA, to foster online media pluralism, and to monitor the adherence of platforms to initiatives aimed at countering harmful content, such as disinformation¹⁷. In this regard, the Board is a critical component in the new governance framework for news content in the platformised public sphere. Its role extends beyond mere monitoring, serving as a forum for the “structuring” of online public discourse, including the strengthening of journalism and media pluralism in the online world. The outcomes of these dialogues on best practices and the activities mentioned in Article 19(1) are to be communicated to the Commission and should be made publicly available when possible. The most notable difference between Article 18 of the Proposal for a Regulation and Article 19 of the EMFA is the inclusion of the possibility to publicise the results of these dialogues. This element further enhances transparency by making this information accessible to civil society, journalists, researchers, and others. The practical impact of the Board on the governance of digital content remains to be seen, but Article 19 of the EMFA lays the groundwork for a system that could help reestablish the role of traditional media and journalism in digital public discourse.

3. The innovations of Article 18 of the EMFA against the previous regulatory tools and criticism of the media privilege provision

The EMFA not only regulates the media system in the European Union’s offline public sphere but also takes a step further by engaging with the

platformised public sphere. It does so by building a mechanism based on a series of safeguards for traditional media in the context of digital governance, as well as by attempting to rebuild – or at least protect – the role of traditional media in the new online context dominated by platforms and private powers. The solution identified by the EMFA, through Articles 18 and 19, is to guarantee a “new” media privilege tailored to the specific characteristics of the platformised public sphere.

This privilege aligns with certain previous provisions of the Code of Practice on Disinformation, which, in both its 2018 and “strengthened” 2022 versions, provided for the prioritisation of content from reliable sources and transparency mechanisms designed to increase the impact of traditional media in online public discourse. The 2018 version of the Code of Practice on Disinformation¹⁸ prescribed, in particular, that platforms should «consistently with Article 10 of the European Convention on Human Rights and the principle of freedom of opinion, invest in technological means to prioritize relevant, authentic, accurate, and authoritative information where appropriate in search, feeds, or other automatically ranked distribution channels»¹⁹. Additionally, the Code included a commitment to develop transparency mechanisms that should facilitate «the assessment of content through indicators of the trustworthiness of content sources, media ownership, and verified identity. These indicators should be based on objective criteria and endorsed by news media associations, in line with journalistic principles and processes»²⁰.

These two measures were reinforced by the 2022 version of the Code²¹, which, concerning the prominence of authoritative sources, recom-

17. Recital 56 of the EMFA is very clear in pointing out that, «Building on the useful role played by ERGA in monitoring compliance by the signatories of the EU Code of Practice on Disinformation, the Board should, at least on a yearly basis, organise a structured dialogue between providers of very large online platforms, representatives of media service providers and representatives of civil society to foster access to diverse offerings of independent media on very large online platforms, discuss experience and best practices related to the application of the relevant provisions of this Regulation, including as regards the moderation processes by very large online platforms, and to monitor adherence to self-regulatory initiatives aimed at protecting users from harmful content, including those which aim to counter disinformation».

18. EUROPEAN COMMISSION 2018.

19. *Ivi*, p. 3.

20. *Ivi*, p. 7.

21. EUROPEAN COMMISSION 2022.

mended implementing «recommender systems designed to improve the prominence of authoritative information and reduce the prominence of disinformation based on clear and transparent methods and approaches for defining the criteria for authoritative information»²². Regarding transparency mechanisms, it stipulated that «Relevant Signatories will make it possible for users of their services to access indicators of trustworthiness – such as trust marks focused on the integrity of the source and the methodology behind such indicators – developed by independent third parties, in collaboration with the news media, including associations of journalists and media freedom organizations, as well as fact-checkers and other relevant entities, that can support users in making informed choices»²³.

Many authors pointed out that the Code of Practice on Disinformation did not contemplate a role for traditional media in the fight against online disinformation. Nevertheless, the two versions of the Code did, to some extent, focus on traditional media, by contemplating trustworthy flagging systems for media actors on digital platforms and by recommending algorithmic systems prioritising authoritative sources. By creating algorithmic or recognition privileges for traditional media, these mechanisms follow the same logic of the EMFA in providing a space in the online public discourse for journalism. While the discipline of the Code of Practice on Disinformation is not as explicit as that

of the EMFA in establishing this privilege mechanism, it follows the same underlying rationale: to guarantee an online space for the main “watchdog of democracy”²⁴, i.e. the media. This approach also echoed the Steering Committee for Media and Information Society of the Council of Europe’s recommendation to States to «make public interest content more prominent, including by introducing new obligations for platforms and intermediaries, and also impose minimum standards such as transparency»²⁵, and the Organization for Security and Co-operation in Europe’s recommendation to «privilege independent quality media and public interest content on their services in order to facilitate democratic discourse»²⁶.

Article 45 of the DSA could incorporate the Code of Practice on Disinformation within the digital governance framework designed by the Regulation, along with the aforementioned mechanisms of algorithmic favour and flagging for media actors. Otherwise, the DSA pays little attention to the issue of media in the new platformised public sphere. Apart from a few references to media freedom and pluralism²⁷, the DSA does not provide any specific discipline for media in the communication ecosystem of digital platforms. The only references to traditional media in the DSA can be found in Recital 47, concerning the terms of service of digital platforms and the need to respect media pluralism²⁸, and Recital 81, concerning the systemic risks that large platforms including media freedom

22. *Ivi*, p. 20.

23. *Ivi*, p. 23.

24. The “vital public-watchdog role of the press” (*Goodwin v. the United Kingdom* judgment of 27 March 1996, Application no. 17488/90) is recognised by a lot of different judgements of the European Court of Human rights (ECtHR). See also: ECtHR, *Bladet Tromsø and Stensaas v. Norway*, judgment of 20 May 1999, Application no. 21980/93.

25. COUNCIL OF EUROPE 2021, p. 2.

26. OSCE 2023, p. 8.

27. Media pluralism which, according to some authors, is linked to Article 18 of the EMFA because «The goal is to ensure “unimpeded” dissemination of media service providers’ content that links Art. 18 to the concept of media pluralism», KŁAFKOWSKA-WAŚNIEWSKA 2024. Besides, Recital 50 of the EMFA states that «Therefore, also in view of users’ right to receive and impart information, where a provider of a very large online platform considers that content provided by such media service providers is incompatible with its terms and conditions, it should duly consider media freedom and media pluralism, in accordance with Regulation (EU) 2022/2065».

28. «When designing, applying and enforcing those restrictions, providers of intermediary services should act in a non-arbitrary and non-discriminatory manner and take into account the rights and legitimate interests of the recipients of the service, including fundamental rights as enshrined in the Charter. For example, providers of very large online platforms should in particular pay due regard to freedom of expression and of information, including media freedom and pluralism». Recital 47, DSA.

and pluralism have to consider²⁹. These recitals could be important elements when interpreting the Regulation, but they do not outline any protection or guarantee system for traditional media on VLOPs.

In the discussion over the DSA proposal, there was much debate over what was called the “non-interference principle” or “media privilege” for traditional media on digital platforms³⁰. Eventually, Amendment 511 to the DSA sought to introduce a media privilege in the regulation of online content: «Intermediary service providers should pay utmost regard to relevant rules applicable to the media and put in place specific procedures, ensuring that the media are promptly informed and have the possibility to challenge any content moderation measure before its implementation»³¹. The amendment partly echoed the content of the current Article 18 of the EMFA but was not adopted. Alongside Amendment 511, Amendment 513 proposed that «In their terms and conditions, providers of intermediary services shall respect the freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms, as enshrined in the Charter, as well as

the rules applicable to the media in the Union»³². This amendment also aimed to make media content more accessible and visible to the public on digital platforms, boosting media pluralism. It was evident that this amendment tried to create a kind of exception for the media in the content moderation systems on VLOPs³³, but also this amendment was not adopted. These two amendments were rejected and were strongly criticised by the academic and journalistic communities involved in fact-checking and countering disinformation³⁴. Critics argued that the amendments would have protected disinformation actors falsely claiming to be media, thereby undermining platforms’ efforts to combat disinformation. This type of media privilege on VLOPs was eventually taken up by the EMFA, and the criticisms that had been made of this privilege in the debate over the proposal of the DSA were reproduced with respect to the EMFA: «All these arguments have been put forward again in the context of the debate around the media privilege»³⁵. In particular, the drafting of the media privilege in the Proposal for a Regulation, Article 17 of the Proposal, has been criticised in several

29. «A second category concerns the actual or foreseeable impact of the service on the exercise of fundamental rights, as protected by the Charter, including but not limited to human dignity, freedom of expression and of information, including media freedom and pluralism, the right to private life, data protection, the right to non-discrimination, the rights of the child and consumer protection. Such risks may arise, for example, in relation to the design of the algorithmic systems used by the very large online platform or by the very large online search engine or the misuse of their service through the submission of abusive notices or other methods for silencing speech or hampering competition». Recital 81, DSA.

30. For a detailed analysis see: PAPAÉVANGELOU 2023, p. 466. Several publishers’ associations were in favour of this exception/privilege: the European News Publishers Association (ENPA), the European Magazine Publishers Association (EMMA), the Association of European Radios (AER), the European Publishers Council (EPC), the European Broadcasting Union (EBU), News Media Europe (NME), and the Association of television and radio sales houses (EGTA). As reported by CESARINI–DE GREGORIO–POLLICINO 2023, p. 7.

31. [A9-0356/511](#).

32. [A9-0356/513](#).

33. «Article 12 should explicitly recognize that the restrictions provided in terms and conditions are drawn up, applied and enforced in compliance with rules applicable to the media, including content standards that serve to protect, for example, minors as well as, more broadly, the freedom of expression and information and the freedom of the media (Article 11 of the Charter). The impact of intermediaries’ T&Cs and decisions taken in relation to lawful media content (e.g. content removal/suspension, suspension of business accounts, re-labelling content suitable for certain age groups, shadow banning, etc) is a very concrete issue, experienced by a variety of media on a variety of platform services regardless of size. The unilateral and unpredictable nature of such decisions represents a hurdle on citizens’ access to information and on media freedom». [A9-0356/513](#).

34. BERTUZZI 2021. These amendments were also described as “good intentions leading to hell” by Věra Jourová (*ibidem*). See also: EU DISINFO LAB 2022; PAILLEUX 2021.

35. CESARINI–DE GREGORIO–POLLICINO 2023, p. 10. For an overview of the debate and some critical remarks: GO-SZTONYI–LENDVAI 2024, p. 72.

ways, which can be grouped into two main strands: the problem of who should be granted the media privilege and the legitimacy of granting a media privilege in the public discourse.

The first strand of criticism focused on the “declaration” required for media entities to obtain the media privilege outlined in Article 17 of the Proposal for a Regulation. According to some authors, that article lacked strict criteria and could result in the acquisition of media privileges by entities involved in disinformation or controlled by authoritarian governments. These criticisms had already been raised during the attempts mentioned above to amend the DSA³⁶. The risks of granting media privileges to entities engaged in disinformation campaigns are addressed in the modified version of Article 18 of the EMFA, which introduces additional requirements for obtaining the media privilege compared to Article 17 of the Proposal for a Regulation. Specifically, independence from entities related to third states and political parties was added to the list of independence requirements. In line with the exclusion from the EU news market of media entities associated with Russia during the Russian-Ukrainian conflict as provided by Regulation (EU) 2022/350 and the fight against disinformation as provided by the Code of Practice on Disinformation, Article 18 of the EMFA seeks to grant media privileges only to those entities that comply with the standards of professional journalism and engage in journalistic practices consistent with the right of EU citizens to be correctly informed. The requirement for media entities seeking this privilege to be subject to regulatory or co-regulatory authorities or bodies, along with the possibility for VLOPs to contact these authorities, adds another layer to the “brake system” in the attribution of the media privilege. As a consequence, the tools to assess a self-declared media’s adherence to the standards of journalism seem present. Confining the media privilege to actors subject to regulatory or co-regulatory mechanisms should further limit the risk of attributing

this privilege to actors engaged in disinformation campaigns. Of course, relying on the monitoring activities of national authorities in the EU Member States does not preclude the attribution of the privilege to media actors that no longer adhere to the parameters of journalism, given the democratic backsliding and rule-of-law crises witnessed in some EU Member States. It is not impossible that some media actors turn into propaganda megaphones for governments with the complicity of a Member State’s regulatory authorities. However, this is a problem that other EMFA provisions seek to address³⁷. Indeed, it would have been excessive to require Article 18 of the EMFA to address this issue as well. From the perspective of attributing media privileges, Article 18 of the EMFA will need to be evaluated in its practical application³⁸. However, the tools to ensure the proper attribution of media “status” appear to be in place.

In this sense, the “content-based” requirements for media entities of Article 18(1) align with Recommendation CM/Rec(2011)7 “on a New Notion of Media”, which is based on parameters such as the intent to act as a media outlet, journalism best practises, editorial control, and professional standards. However, Article 18 of the EMFA fails to address the transformations journalism has undergone in the digital age and to expand the range of media subjects beyond classical publishers, as was attempted by Recommendation CM/Rec(2011)7³⁹. The approach in Article 18 of the EMFA appears to guarantee this privilege only to media entities subject to regulatory or co-regulatory regimes, i.e., traditional media companies.

Regarding the risk of favouring disinformation actors, it should also be noted that Article 18 of the EMFA does not apply to systemic risk, including disinformation. Media privilege does not apply to content moderation conducted by VLOPs in compliance with «obligations pursuant to Articles 28, 34, and 35 of Regulation (EU) 2022/2065 and Article 28b of Directive 2010/13/EU or their obligations relating to illegal content under Union law»

36. EU DISINFO LAB 2021.

37. The enforcement of EMFA is something that many authors have discussed: BAYER–CSERES 2023.

38. A series of interesting considerations can be read in relation to Article 17 of the Proposal for a Regulation in BARATA 2022.

39. Council of Europe, Recommendation CM/Rec(2011)7 of the Committee of Ministers to Member States on a New Notion of Media, 21 September 2011.

(Art. 18(4) of the EMFA). Recital 51 of the EMFA makes this point explicit, stating: «This Regulation should not affect the obligations of providers of very large online platforms to take measures against illegal content disseminated through their services, to take measures in order to assess and mitigate systemic risks posed by their services, for example through disinformation». After mitigating the risks of granting privilege to actors involved in disinformation campaigns, a reasonable balance appears to have been achieved between the need to counter disinformation and the need to protect traditional media from potential unfair censorship by platforms⁴⁰. In this perspective, Article 18 of the EMFA seems well-equipped to avoid becoming a vehicle for disinformation.

The second strand of criticism pertains to a deeper constitutional issue regarding the very legitimacy of a media privilege, questioning why such a privilege should be guaranteed to media in the online public sphere⁴¹. This criticism reflects a more profound set of constitutional concerns, often influenced by the US approach to freedom of expression⁴². In the US legal system, the dominant interpretation of the First Amendment does not recognise any autonomy for the Press Clause separate from the Speech Clause⁴³, encompassing all expressions under the umbrella of political free speech. As a result, no special protections exist for the press at the federal level, and no discrimination can be made between different speakers⁴⁴. This constitutional approach precludes recognising a special role for the press in the public discourse,

although, in practice, this primacy has been constructed in alignment with the media system. On the contrary, in the European Union system and in many of its Member States the exact opposite can be affirmed⁴⁵: «The US Supreme Court has tended to resist special institutional protection for journalism or the media, but in Europe, the role of the press in a democracy justifies such support, including through positive interventions by the state»⁴⁶. This was also one of the foundational assumptions of the Committee of Ministers of the Council of Europe recommendation on new forms of media: «Since their emergence as a means of mass communication, media have been the most important tool for freedom of expression in the public sphere, enabling people to exercise their right to seek and receive information. Media animate and provide a space for public debate. Media offer comment and opinion as part of political dialogue, contribute to setting the political agenda and the shaping of public opinion, and they often seek to promote certain values. Media facilitate the scrutiny of public and political affairs and private or business-related matters, thereby increasing transparency and accountability»⁴⁷. Consequently, «Historically, media regulation has been justified by and graduated having regard to its potential high impact on society and on individual rights; regulation has also been a means of managing scarce resources in the public interest. Given their importance for democracy, media have been the subject of extensive Council of Europe standard-setting activity. The purpose has been to ensure *the highest protection of*

40. «[T]he fight against disinformation should not completely overshadow the fact that the media found themselves in a worryingly subordinate position in relation to VLOPs and that Article 17 of the EMFA is the only mechanism that seeks to promote the principle that technology companies with little or no editorial responsibility should not censor journalism». NENADIĆ–BROGI 2023.

41. As well summarised by the question «Above all, how will the new legislation be applied in practice and how will it work to ensure that it neither undermines the equality of speech and democratic debate nor endangers vulnerable groups?». ALLIOUI 2024.

42. It is no coincidence that references to the risk of “undermining the equality of free speech” originate from US NGOs: COLLINGS–SCHMON 2023.

43. WEST 2014.

44. Outside the commercial speech category, an “unrestrained epistemic egalitarianism” (POST 2013, p. 32) is in fact established under the First Amendment. HORWITZ 2012, p. 471.

45. For a recognition with also references to various national legal systems: CAPPELLO 2017.

46. TAMBINI 2021, p. 523.

47. Council of Europe, Recommendation CM/Rec(2011)7 of the Committee of Ministers to Member States on a New Notion of Media, 21 September 2011, p. 5.

media freedom and to provide guidance on duties and responsibilities»⁴⁸ (emphasis added).

Employing the European Convention on Human Rights (ECHR) system as a reference, which, according to Article 52(3) of the European Union Charter of Fundamental Rights (EU CFR), serves as a parameter for interpreting fundamental rights within the European Union, including Article 11 of the EU CFR, we can detect a different European constitutional approach compared to the US. In Europe, traditional media have been recognised as “watchdogs of democracy”⁴⁹, meaning their activities contribute to holding political power accountable and to accurately transmitting news to citizens⁵⁰. As such, they are considered deserving of special protection in the regulation of public discourse. Even within the European Union, beyond the EMFA, the role of the press and journalism has been recognised as deserving of special protection, as evidenced by various exceptions

provided in many regulations for the journalistic media, such as Article 85 of the GDPR⁵¹.

The advent of the digital world has, of course, disrupted the communicative paradigm on which news transmission in the public sphere was based, leading to an epochal change in the production of culture with the «transformation of audiences (...) into practitioners»⁵². In other words, the new tools of the digital world «radically alter the previously predominant pattern of communication in the public sphere by empowering all potential users in principle to become independent and equally entitled authors»⁵³. This structural change in the production of culture has also impacted news production, leading to a crisis of journalism in the United States, where no regulatory instruments exist to legislatively or judicially guarantee a presence for traditional media online⁵⁴. Nevertheless, private actors, such as platforms, have attempted to ensure this space for traditional media since

48. *Ivi*.

49. This role is also carried out through media privileges such as journalists’ sources protection: «The Court reiterates that freedom of expression constitutes one of the essential foundations of a democratic society and that the safeguards to be afforded to the press are of particular importance. The protection of journalistic sources is one of the cornerstones of freedom of the press. Without such protection, sources may be deterred from assisting the press in informing the public about matters of public interest. As a result, the vital public-watchdog role of the press may be undermined, and the ability of the press to provide accurate and reliable information may be adversely affected». ECtHR, *Weber and Saravia v. Germany*, Application no. 54934/00.

50. For example: ECtHR, *Pedersen and Baadsgaard v. Denmark* (Application no. 49017/99), 2004; protection is to be extended to non-professional journalists, such as regular opinion writers: ECtHR, *Falzon v. Malta*, 2018, (Application no. 45791/13).

51. Art. 85 of the GDPR (EU Regulation 2016/679): «Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression». Already the pre-GDPR Directive 95/46/EC provided in Article 9: «Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression». In addition, media privileges were also evident in relation to Article 15 of the Copyright Directive (Directive (EU) 2019/790) or the special focus on the protection of journalistic material in Recital 12 of Regulation (EU) 2021/784 on online terrorist content.

52. SACCO 2011, p. 7.

53. HABERMAS 2022, p. 159.

54. «The media exemption discloses further difficulties with the law now under consideration. There is no precedent supporting laws that attempt to distinguish between corporations which are deemed to be exempt as media corporations and those which are not. “We have consistently rejected the proposition that the institutional press has any constitutional privilege beyond that of other speakers.” (...) With the advent of the Internet and the decline of print and broadcast media, moreover, the line between the media and others who wish to comment on political and social issues becomes far more blurred». *Citizens United v. FEC*, 558 U.S. 130 S. Ct. 876 (2010).

they are not “state actors” or “common carriers”⁵⁵ bound by First Amendment rules and can therefore “discriminate” between different speakers in their private spaces⁵⁶. In the European Union, this structural change in news content production has led to various queries about the magnitude of this transformation. Eventually, it has led, as mentioned above, to the enactment of soft- and hard-law instruments attempting to guarantee the presence of media and journalism in the online public discourse. After all, if the European Court of Human Rights (ECtHR) has recently acknowledged the extension of the watchdog of democracy role to so-called “citizen journalism”⁵⁷, the Council of Europe institutions have similarly emphasised the need to strengthen the role of traditional journalistic media in the platformised public sphere⁵⁸. In a 2022 recommendation, the Committee of Ministers pointed out the need to ensure both the availability of journalism products⁵⁹ and their prioritisation in the digital world⁶⁰. The media privilege in Article 18 of the EMFA responds to this constitutional logic and aligns with the provisions of the Code of Practice on Disinformation

on granting a special space to media in the online public discourse. Thus, Article 18 of the EMFA reproduces and reflects a European constitutional approach towards media that has consistently “guaranteed” a special role for media entities in the public sphere. The EMFA simply attempts to replicate part of this approach in the digital public sphere: «Media service providers that exercise editorial responsibility over their content play a key role in the distribution of information and in the exercise of the right to receive and impart information online. When exercising such editorial responsibility, media service providers are expected to act diligently and provide information that is trustworthy and respectful of fundamental rights, in line with the regulatory requirements or co-regulatory or self-regulatory mechanisms to which they are subject in the Member States» (Recital 50 of the EMFA). Attributing media privilege to traditional media thus seems in line with the European constitutional paradigm of freedom of expression⁶¹.

Regarding the media privilege of the EMFA, however, there may be issues about the restricted

55. Even in its recent ruling on the Florida and Texas laws, the Supreme Court did not frame digital platforms as common carriers: *Moody v. NetChoice, LLC and NetChoice, LLC v. Paxton*, 603 U.S. ____ (2024).

56. Think of the fact-checking done with traditional media on Donald Trump’s Twitter statements; or the emergency communication implemented during the pandemic period relying heavily on the products of traditional media and journalism.

57. ECtHR, *Cengiz and Others v. Turkey*, Applications nos. 48226/10 and 14027/11, 2016.

58. «All types of media, in their increasing variety, have an important role to play in fulfilling the promise of journalism at a time when the ever-growing amount of information accessible to large audiences, coupled with the difficulty of determining the sources of all this information, stretches the ability of societies to assess its accuracy and reliability. Journalistic practices that uphold this role, and the values and principles set forth above, should be acknowledged as a public good», Recommendation CM/Rec(2022)4 of the Committee of Ministers to Member States on promoting a favourable environment for quality journalism in the digital age.

59. «Digital media distribution channels and gateways with curated or sponsored content now influence the access to and the findability of quality content, including from public service media, through their personalised selection and recommendations based on users’ expressed or inferred preferences. States, in collaboration with online platforms and other relevant internet intermediaries, media organisations and other key stakeholders that represent the whole diversity of society, should address the challenges related to the online distribution of public interest media content and develop appropriate regulatory responses to ensure that such content is universally available, easy to find and recognised as a source of trusted information by the public», *ivi*.

60. «Prioritisation of public interest journalism: effective access to quality journalism should be supported by independent and transparent self-regulatory media initiatives, open to multi-stakeholder participation, that develop criteria for identifying reliable content», *ivi*.

61. In its “media freedom” sub-category: «media freedom is partly a derivative right from freedom of expression, and partly a self-standing right. For adhering to its duties and responsibilities, media freedom affords particular privileges to the media, which do not apply to freedom of expression in general: the media speech privilege and the protection of the media as an institution», OSTER 2015.

attribution of this privilege, especially given the attempts to broaden the recognition of journalistic actors and watchdogs of democracy in Europe. The aforementioned Recommendation CM/Rec(2011) of the Committee of Ministers of the Council of Europe acknowledged the importance of “journalistic” actors not traditionally categorised as media, which seems to be a challenge that Article 18 of the EMFA has not addressed. This is despite the fact that within the European Union, case law has increasingly begun to consider the role of journalists more broadly⁶². However, Article 18 of the EMFA does not extend the recognition of the media privilege to “citizen journalism” (or NGOs⁶³) or the other new forms of internet journalism⁶⁴ protected under ECtHR jurisprudence. Thus, the media privilege under Article 18 of the EMFA may be more questionable due to its limited attribution to “traditional” media⁶⁵ alone, rather than from the perspective of the legitimacy of a media privilege itself. However, extending this privilege to entities not “formally” categorised as traditional media, and thus not regulated by national authorities or bodies etc., would undoubtedly have made the attribution of this privilege more problematic. It would have increased the risks of granting it to disinformation agents, aggravated the controls imposed on VLOPs, and complicated the mechanisms of representation in the Board and the structured dialogues. Although part of the literature has raised concerns about the exclusion of new media actors and the potential discrimination against

them compared to traditional media, extending the privilege to these new actors would have been challenging on a practical level⁶⁶. However, in this context, as mentioned earlier, even the mere extension of the privilege to traditional media may be problematic in the context of democratic regression and rule of law crisis in some EU Member States⁶⁷. Such a provision could theoretically protect media entities that have abandoned journalism standards, such as Fox News or FranceSoir, which have turned into agents of populist disinformation/conspiracy theories⁶⁸. Monitoring media adherence to journalism and professional standards is left to national authorities by Article 18 of the EMFA. In contexts of democratic backsliding, this provision could therefore be problematic, but it cannot be a responsibility of Article 18 of the EMFA to address this issue. Instead, it has to be dealt with within the broader framework of the EMFA.

4. Final Remarks

The review of Articles 18 and 19 of the EMFA demonstrates that the adjustments made to the media privilege mechanism, particularly in response to criticisms of Article 17 of the previous Proposal for a Regulation, should alleviate many of the concerns previously raised. The media privilege established by the EMFA is clearly designed to protect spaces for journalism within the online public sphere, particularly on VLOPs. The attribution of media privilege depends heavily on the recognition of media entities by the national regu-

62. See the extension of exemptions for the processing of personal data (Art. 9 Directive 95/46/EC) to anyone engaged in “journalistic activities”: CJEU, *Sergejs Buivids v. Datu valsts inspekcija*, Case C-345/17; CJEU, *Satakunnan Markkinapörssi and Satamedia*, C-73/07.

63. ECtHR, *Animal Defenders v. the United Kingdom*, Application no. 48876/08.

64. See: ECtHR, *Delfi v. Estonia*, App. 64669/09; ECtHR, *Magyar Helsinki Bizottság v. Hungary*, Application no. 18030/11.

65. Cf. SEIPP-FATHAIGH-VAN DRUNEN 2023, p. 39. Part of the criticism regarding transparency in the attribution of the privilege has been addressed in the new version of Article 18 of the EMFA, which, as discussed above, introduces enhanced transparency mechanisms.

66. CESARINI-DE GREGORIO-POLLICINO 2023, p. 16, which stress how «in principle, in order to avoid legal challenges, the media privilege should adopt a functional and broader MSP definition. However, such an adjustment would substantially expand the range of potential beneficiaries, thereby increasing the risks of circumventions by malicious actors. Moreover, the process of verification by VLOPs of the self-declarations submitted by potential beneficiaries would become extremely cumbersome if not impossible to implement, taking into account the fluid and fast-changing landscape of media actors in the digital space».

67. See the sections on *Media pluralism and media freedom* of EUROPEAN COMMISSION 2024.

68. CESARINI-DE GREGORIO-POLLICINO 2023, p. 9.

latory authorities in the EU Member States. In this sense, the provision also assigns responsibilities to VLOPs, allowing them to contact the relevant national regulatory authorities if they have doubts about the accuracy of the self-declaration.

However, Article 18 of the EMFA limits the attribution of media privilege to traditional media, excluding those new forms of journalism that have been recognised by the ECtHR caselaw. Despite the criticism of the provision, «proposals like the non-interference principle are far from perfect but they are erring towards the right direction»; indeed addressing «how platforms moderate content, especially the kind that is vital for democratic deliberation like news, is timely considering the ongoing structural transformation of the public sphere. Who gets to partake in its governance is crucial to the public interest»⁶⁹. Given the practical difficulties in extending media privilege to other forms of journalism and other democratic watchdogs, granting this privilege to traditional media can be justified by the fact that «the media organisations still provide the key infrastructure for journalism to operate in a professional way»⁷⁰. Since it is crucial to grant this privilege to actors who operate under specific professional standards and adhere to the practices of ethical and responsible journalism, the solution provided by Article 18 of the EMFA appears to be the only viable option. Nonetheless, there could be issues with granting the privilege to media subjects that meet formal requirements but fail in substance, such as those that

do not adhere to the practices of journalism or are not independent from governments. For example, media entities subject to regulatory authorities in Member States experiencing democratic backsliding and rule-of-law issues might, in practice, act as propaganda tools for governments. However, it seems unreasonable to expect a provision designed to protect media in the online environment to also address such broad issues. These concerns are better addressed by other articles within the EMFA. The strengthening of media protections under the general provisions of the EMFA will likely have a positive impact on the online realm as well.

Ultimately, the enactment of Article 18 of the EMFA strengthens the EU's paradigm of freedom of expression with respect to the media's special role in constitutional democracies. It also represents the missing piece in the digital governance framework envisioned by the DSA, ensuring a stronger media presence in the digital public sphere. Of course, these theoretical considerations have to be tested in the actual implementation of Article 18 of the EMFA. The transparency requirements embedded in this provision and in Article 19 of the EMFA will enable researchers and policymakers to evaluate the effectiveness of this public policy and contribute to its potential reformulation or improvement. In the meantime, the media privilege outlined in Articles 18 and 19 of the EMFA aims to restore the role of journalism in the platformised public sphere and ensure its continued contribution to public discourse.

References

- S.A. ALLIOUI (2024), *EU Media Freedom Act: the convolutions of the new legislation*, EU Law Analysis, 6 June 2024
- J. BARATA (2022), *Protecting Media Content on Social Media Platforms*, in “Verfassungsblog: On Matters Constitutional”, 25 November 2022
- J. BAYER, K. CSERES (2023), *Without Enforcement, the EMFA Is Dead Letter*, in “Verfassungsblog: On Matters Constitutional”, 13 June 2023
- L. BERTUZZI (2021), *Media exemption ruled out in DSA negotiations, but could return*, Euractiv, 2021
- M. CAPPELLO (ed.) (2017), *Journalism and Media Privilege*, IRIS Special, European Audiovisual Observatory, 2017

69. PAPAÉVANGELOU 2023, p. 476.

70. NENADIĆ–BROGI 2023.

- P. CESARINI, G. DE GREGORIO, O. POLLICINO (2023), *The Media Privilege in the European Media Freedom Act*, in “MediaLaws”, 2023
- P. COLLINGS, C. SCHMON (2023), *EU Media Freedom Act: A Media Privilege in Content Moderation Is a Really Bad Idea*, Electronic Frontier Foundation, 12 July 2023
- COUNCIL OF EUROPE (2021), *Guidance Note on the Prioritisation of Public Interest Content Online adopted by the Steering Committee for Media and Information Society (CDMSI) at its 20th plenary meeting*, 1-3 December 2021
- EU DISINFO LAB (2022), *DSA: The Proposed Amendments to Article 12 and Recital 38 Should Be Rejected*, 2022
- EU DISINFO LAB (2021), *Fact-Checkers and Experts Call on MEPS to Reject a Media Exemption in the DSA*, 2021
- EUROPEAN COMMISSION (2024), *Rule of Law Reports of the European Commission*, 24 July 2024
- EUROPEAN COMMISSION (2022), *2022 Strengthened Code of Practice on Disinformation*, 2022
- EUROPEAN COMMISSION (2018), *EU Code of Practice on Disinformation*, 2018
- G. GOSZTONYI, F. GERGELY LENDVAI (2024), *Could European Media Freedom Act Solve the Problems of Traditional Media’s Content in the Online Sphere?*, in “Informatization Policy”, vol. 31, 2024, n. 1
- J. HABERMAS (2022), *Reflections and Hypotheses on a Further Structural Transformation of the Political Public Sphere*, in “Theory, Culture & Society”, vol. 9, 2022, n. 4
- P. HORWITZ (2012), *The First Amendment’s Epistemological Problem*, in “Washington Law Review”, vol. 87, 2012, n. 2
- K. KŁAFKOWSKA-WAŚNIEWSKA (2024), *Taking Extra Care of the Media? Media Content Moderation under the European Media Freedom Act*, in “VerfassungsBlog on Matter Constitutional”, 16 July 2024
- M. MONTI (2018), *Automated Journalism and Freedom of Information: Ethical and Juridical Problems Related to AI in the Press Field*, in “Opinio Juris in Comparatione”, vol. 1, 2018, n. 1
- I. NENADIĆ, E. BROGI (2023), *Why News Media Need Article 17 of the European Media Freedom Act*, Centre for Media Pluralism and Freedom, 16 November 2023
- T.M. NICHOLS (2017), *The Death of Expertise: The Campaign Against Established Knowledge and Why it Matters*, Oxford University Press, 2017
- P. ORTOLANI (2022), *The Digital Services Act, Content Moderation and Dispute Resolution*, in “Giustizia Consensuale”, 2022, n. 2
- OSCE (2023), *Joint Declaration on Media Freedom and Democracy*, 2 May 2023
- J. OSTER (2015), *Media Freedom as a Fundamental Right*, Cambridge University Press, 2015
- N. PAILLEUX (2021), *Don’t Open the Door to Disinformation: Reject the Media Exemption in the DSA*, in “CheckFirst”, December 2021
- C. PAPAEVANGELOU (2023), *‘The Non-Interference Principle’: Debating Online Platforms’ Treatment of Editorial Content in the European Union’s Digital Services Act*, in “European Journal of Communication”, vol. 38, 2023, n. 5
- R.C. POST (2013), *Democracy, Expertise, and Academic Freedom: A First Amendment Jurisprudence for the Modern State*, Yale University Press, Reprint edition, 2013
- P.L. SACCO (2011), *Culture 3.0: A New Perspective for the EU 2014-2020 Structural Funds Programming*, EENC Paper, April 2011

- M. SEELIGER, S. SEVIGNANI (2022), *A New Structural Transformation of the Public Sphere? An Introduction*, in “Theory, Culture & Society”, vol. 39, 2022, n. 4
- T. SEIPP, R.Ó. FATHAIGH, M. VAN DRUNEN (2023), *Defining the ‘Media’ in Europe: Pitfalls of the Proposed European Media Freedom Act*, in “Journal of Media Law”, vol. 15, 2023, n. 1
- D. TAMBINI (2021), *What Is Journalism? The Paradox of Media Privilege*, in “European Human Rights Law Review”, vol. 5, 2021
- M.Z. VAN DRUNEN et al. (2023), *What Can a Media Privilege Look like? Unpacking Three Versions in the EMFA*, in “Journal of Media Law”, vol. 15, 2023, n. 2
- S.R. WEST (2014), *Press Exceptionalism*, in “Harvard Law Review”, vol. 127, 2014, n. 8



LILIANA CILIBERTI

DSA e EMFA: speciale responsabilità delle piattaforme online e tutela della libertà dei media

Il margine di discrezionalità che viene lasciato alle piattaforme online di dimensioni molto grandi nei confronti dei servizi di media presenti sui loro servizi è troppo ampio e solleva preoccupazioni. Tali preoccupazioni non sono superate dalla previsione del cd. *media privilege*, e cioè dall'obbligo a carico delle piattaforme di una previa interlocuzione con gli editori dei servizi di media prima di procedere all'applicazione di qualsiasi limitazione, dal momento che il *media privilege* è soggetto ad alcune importanti deroghe. Il presente contributo ha l'obiettivo di fornire riflessioni a sostegno di un'interpretazione restrittiva di tali deroghe. Un celere intervento da parte delle istituzioni, nazionali ed europee, che precisi i margini di intervento delle piattaforme nei confronti dei servizi degli editori di media, potrebbe evitare quella sorta di delega alle piattaforme di poteri pubblici che il nuovo contesto normativo sembrerebbe avallare.

*Libertà e pluralismo dei media – Indipendenza editoriale – Media privilege – Principio di legalità
Delega di poteri*

DSA and EMFA: special responsibility for online platforms and safeguarding media freedom

The margin of discretion granted to very large online platforms with respect to media services available on their platforms is excessively broad and raises concerns. These concerns are not alleviated by the so-called media privilege, which requires platforms to engage in prior consultation with media service providers before applying any limitations, as this privilege is subject to many significant exceptions. My written contribution aims to provide some thoughts on a restrictive interpretation of these exceptions. A prompt intervention by national and European institutions to clarify the scope of platforms' actions towards media service providers could prevent a sort of delegation of public powers to the platforms that the new regulatory framework seems to endorse.

*Media freedom and pluralism – Editorial independence – Media privilege – Principle of legality
Delegation of powers*

L'Autrice è consulente legale e cultrice della materia del Corso "Informazione, diritti e mercati digitali", Laurea magistrale di Comunicazione pubblica e d'impresa, Facoltà di Scienze politiche, economiche e sociali, Università degli Studi di Milano

Questo contributo fa parte della sezione monografica *EMFA under the spotlight: towards a common regulatory framework to foster media pluralism?* a cura di Elda Brogi

SOMMARIO: 1. Premessa. – 2. Gli obiettivi dell’EMFA e il suo art. 18. – 2.1. *La procedura ex ante e ex post del media privilege*. – 2.2. *I diritti fondamentali dei fornitori di servizi di media*. – 3. I servizi di media. – 4. Le piattaforme online e le piattaforme televisive. – 5. Analisi delle norme e dei loro rapporti. – 5.1. *Gli artt. 28, 34 e 35 del DSA*. – 5.2. *L’art. 28 ter della Direttiva SMA*. – 5.3. *Gli obblighi relativi ai contenuti illegali*. – 5.4. *Il rapporto tra DSA e EMFA*. – 5.5. *La Direttiva SMA e l’EMFA*. – 6. La speciale responsabilità dei fornitori di VLOP. – 7. Conclusioni.

1. Premessa

L’oggetto della presente analisi riguarda l’art. 18, par. 4, ult. co. dello European Media Freedom Act¹ che prevede le ipotesi di inapplicabilità del cd. *media privilege*, e cioè dell’obbligo di previo contraddittorio tra fornitori di piattaforme online di dimensioni molto grandi e fornitori di servizi di media, nel caso in cui i primi «sospendono la fornitura dei propri servizi in relazione a contenuti forniti da un fornitore di servizi di media o limitano la visibilità di tali contenuti conformemente ai loro obblighi

a norma degli articoli 28, 34 e 35 del Regolamento (UE) 2022/2065 e dell’articolo 28 *ter* della direttiva 2010/13/UE, o agli obblighi relativi ai contenuti illegali che incombono loro in forza del diritto dell’Unione»².

Ai sensi dell’EMFA, il “*media privilege*”, noto anche come “*esenzione media*”, consiste in una procedura di garanzia a tutela dei Servizi di Media (MS – *Media Service*) che impedisce ai fornitori di piattaforme online di dimensioni molto grandi (VLOP – *Very Large Online Platform*)³ di

1. Regolamento (UE) [2024/1083](#) dell’11 aprile 2024 che istituisce un quadro comune per i servizi di media nell’ambito del mercato interno e che modifica la direttiva 2010/13/UE (regolamento europeo sulla libertà dei media). In questo contributo, il Regolamento sarà indicato anche con l’acronimo “EMFA” (*European Media Freedom ACT*). L’altro regolamento europeo oggetto di analisi in questo contributo è il Regolamento (UE) [2022/2065](#) del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), che sarà indicato di seguito anche con l’acronimo “DSA” (*Digital Services Act*).
2. L’art. 18, par. 4, co. 1-2 dell’EMFA prevede che «Il fornitore di una piattaforma online di dimensioni molto grandi che intenda adottare la decisione di sospendere la fornitura dei propri servizi di intermediazione online in relazione a contenuti forniti da un fornitore di servizi di media [...] o la decisione di limitare la visibilità di tali contenuti, sulla base del fatto che tali contenuti sono incompatibili con i propri termini e condizioni, provvede, prima che tale decisione di sospendere o limitare la visibilità abbia effetto, a: a) comunicare al fornitore di servizi di media in questione la motivazione [...]; e b) dare al fornitore di servizi di media la possibilità di rispondere alla motivazione [...] entro 24 ore [...] o, in caso di crisi [...], entro un termine più breve [...]. Se, a seguito o in assenza di una risposta [...] decide di sospendere o limitare la visibilità, ne informa senza indebito ritardo il fornitore di servizi di media interessato.». Seguono a tali previsioni quelle di cui all’ultimo capoverso, riportate nel testo di questo contributo.
3. Ai sensi del DSA, *Very Large Online Platform* sono le piattaforme online «che hanno un numero medio mensile di destinatari attivi del servizio nell’Unione pari o superiore a 45 milioni [...]» (art. 33, par. 1). In considerazione del loro ruolo specifico, portata più ampia e impatto maggiore, sono previsti obblighi supplementari rispetto a quelli applicabili a qualsiasi fornitore di servizi intermediari (artt. 11-15 del DSA), di memorizzazione (artt.

interferire *inaudita altera parte* (appunto, senza contraddittorio) con i contenuti dei fornitori di MS (MSP – *Media Service Provider*)⁴ che gli stessi fornitori di VLOP (VLOPP – *VLOP Provider*) dovessero ritenere in contrasto con le loro condizioni generali.

Infatti, si richiede un'interazione con i MSP prima che la decisione dei VLOPP «di sospendere o limitare la visibilità abbia effetto»⁵.

Il *media privilege* è accompagnato da alcune garanzie di trasparenza e da meccanismi di reclamo attivabili dai MSP “qualificati” ai sensi dell'art. 18⁶.

Nel corso di questa analisi verranno esaminate le norme rilevanti e il rapporto tra di esse, considerando l'obiettivo dell'EMFA di rafforzare l'indipendenza e l'autonomia editoriale dei MSP rispetto a qualsiasi interferenza illegittima, sia essa esercitata da un potere pubblico o privato, e alla luce della Carta dei diritti fondamentali dell'Unione europea (“Carta”)⁷, che espressamente include la libertà e l'indipendenza dei media tra i suoi diritti fondamentali⁸ e che prevede che «Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla [...] Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà»⁹.

L'obiettivo è comprendere se vi sia una lettura delle norme che salvaguardi concretamente il *media privilege* voluto dall'EMFA.

Nell'ambito delle considerazioni che verranno svolte, si terrà conto anche dell'esperienza nazionale dei Servizi di Media Audiovisivi (da intendersi come inclusivi dei Servizi di Media solo audio)¹⁰ (SMA) con particolare riferimento alla loro relazione con le piattaforme televisive. Infatti, in tale pluriennale esperienza si sono posti problemi di fondo che si ripropongono ora, e cioè la necessità di preservare l'autonomia degli editori rispetto a soggetti “intermediari”.

Questa esperienza dimostra che, con l'introduzione delle tecnologie digitali di trasmissione, che hanno ampliato la diffusione e l'accessibilità ai SMA¹¹, nonché il numero di attori coinvolti (tra cui piattaforme televisive, operatori di rete, fornitori di servizi di accesso condizionato e editori televisivi), il mantenimento della distinzione dei rispettivi ruoli, e in particolare dell'autonomia editoriale dei media rispetto agli altri attori, non solo non ha portato al fallimento del sistema, ma ha piuttosto favorito il pluralismo dei servizi di media audiovisivi.

Il successo di tale modello è da ricondurre alle prescrizioni normative e alle garanzie

16-17 del DSA), di piattaforme online (artt. 19-28 e, nel caso consentano la conclusione di contratti a distanza, artt. 29-32 del DSA).

4. Per la definizione di Fornitori di Servizi di Media, ai sensi dell'EMFA, si veda successivo paragrafo 3.

5. Art. 18, par. 4, dell'EMFA.

6. V. *infra* paragrafo 2.1.

7. Carta dei diritti fondamentali dell'Unione europea, in G.U.C.E. del 18 dicembre 2000/C, 364/01.

8. In base all'art. 51, par. 1, della Carta, le istituzioni e gli organi dell'Unione europea, nonché gli Stati membri rispettano i diritti e osservano i principi, nel rispetto dei principi di legalità, proporzionalità e sussidiarietà. (V. a riguardo, CAVASINO 2020, p. 567). Sulla diversa “portata” degli effetti dei diritti e dei principi della Carta v. *infra* nota 73.

9. Art. 52 della Carta.

10. La Direttiva sui Servizi di Media Audiovisivi non si occupa dei servizi di media solo audio, mentre a livello nazionale la disciplina applicabile ai SMA potrebbe essere estesa a questi ultimi servizi. V. il d.lgs. 25 marzo 2024, n. 50 che include i servizi radiofonici nella nozione di “fornitore di servizio di media audiovisivo” (art. 3, co. 1, lett. d)).

11. Si pensi ai canali televisivi *all news* che sono sviluppati grazie alle opportunità offerte dalle tecniche digitali di trasmissione, quali ad esempio Sky TG24, RAI News, TGCOM24 HD, CNN.

regolamentari¹² applicabili ai SMA, quali unici e soli soggetti responsabili dei contenuti dagli stessi selezionati e organizzati in un palinsesto televisivo o in un catalogo¹³.

Si tratta di norme che tutelano la collettività e l'individuo e che, al contempo, preservano l'autonomia e l'indipendenza editoriale¹⁴.

Tali prescrizioni e garanzie sono quelle sostanzialmente richieste ai sensi dell'art. 18, par. 1 lett. d) dell'EMFA¹⁵ per la qualificazione di un MSP ai fini del beneficio del "*media privilege*", e la loro eventuale assenza in uno Stato membro comporta

l'inapplicabilità del *media privilege* ai MSP soggetti alla sua giurisdizione¹⁶.

In sintesi, il *media privilege*, così come disciplinato nell'EMFA, ossia la temporanea sospensione delle attività di rimozione o di limitazione della visibilità di contenuti da parte dei VLOPP, rappresenta la misura minima necessaria per la salvaguardia dei MSP "qualificati", anche alla luce del principio di legalità sancito dalla Carta.

Rimetterlo in discussione in sede di interpretazione ed applicazione dell'art. 18, par. 4, ult. co. dell'EMFA, potrebbe rischiare di porre di fatto nel

12. Il termine "regolamentari" si riferisce non solo alla normativa di settore, ma anche alla coregolamentazione e all'autoregolamentazione, in conformità alla lett. d, par. 1, dell'art. 18 dell'EMFA. La formulazione di quest'ultimo articolo è volutamente ampia, considerando che, ad esempio in Italia, le pubblicazioni giornalistiche di un editore che non sono incluse in un servizio di media audiovisivo non sono necessariamente soggette alla regolamentazione di Autorità di settore, bensì a quella di organismi professionali.

13. In Italia, la disciplina di settore applicabile ai SMA è quella contenuta nel Testo unico per la fornitura di servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato approvato con d.lgs. 208/2021, come modificato dal d.lgs. 50/2024 ("TUSMA"). Al TUSMA si aggiungono le regolamentazioni dettate dall'Autorità per le Garanzie nelle Comunicazioni ("AGCOM"), nonché i codici di coregolamentazione e autoregolamentazione previsti dallo stesso TUSMA o dalla regolamentazione AGCOM. Su tali codici, v. CILIBERTI-SANFILIPPO 2024, p. 57 ss. Potrebbe, inoltre, ritenersi ancora applicabile l'art. 30 della l. 6 agosto 1990, n. 223 (sentenza 22 giugno – 12 luglio 2021, n. 150). Per la disciplina sugli editori di prodotti giornalistici, v. la legge sulla stampa 8 febbraio 1948, n. 47, nonché il «Testo unico dei doveri del giornalista», del 22 gennaio 2019. Ove questi ultimi siano fornitori di SMA si applicano anche le norme del TUSMA. Inoltre, rilevano le norme del Regolamento UE n. 679/2016 sulla protezione dei dati personali e il Codice Privacy di cui al d.lgs. 196/2003 e s.m.i., nonché quelle regolanti fattispecie di reato. Per un elenco delle fattispecie di reato attinenti alla professione giornalistica, v. il sito dell'Ordine dei giornalisti – Consiglio nazionale. V. anche CUNIBERTI 2017; MALAVENDA-MELZI D'ERIL-VIGEVANI 2012.

14. Il fornitore di SMA è individuato proprio per la sua responsabilità editoriale nella selezione dei singoli contenuti e la loro organizzazione in un palinsesto televisivo o in un catalogo. V. successivo paragrafo 3. L'autonomia editoriale risalta nelle norme sulla sponsorizzazione (art 46, co. 1, lett. a del TUSMA), nonché in quelle sul *product placement* (art. 48, co. 3, lett. a del TUSMA).

15. Si prevede, infatti, che il beneficio del *media privilege* richiede, tra le altre cose, la dichiarazione da parte dei MSP «che sono soggetti a prescrizioni normative per l'esercizio della responsabilità editoriale in uno o più Stati membri e alla supervisione di un'autorità o di un organismo competente nazionale di regolamentazione, o aderiscono a un meccanismo di coregolamentazione o autoregolamentazione che disciplina le norme editoriali, ampiamente riconosciuto e accettato nel pertinente settore dei media in uno o più Stati membri» (art. 18, par. 1, lett. d, dell'EMFA). Tale dichiarazione è particolarmente rilevante tanto che «In caso di ragionevole dubbio circa la conformità del fornitore di servizi di media al primo comma, lettera d), il fornitore di una piattaforma online di dimensioni molto grandi chiede conferma in merito all'autorità o all'organismo nazionale di regolamentazione competente o al pertinente meccanismo di coregolamentazione o autoregolamentazione». (art. 18, par. 1, ult. co., dell'EMFA).

16. In base all'art. 18, par. 1, dell'EMFA, i VLOPP devono mettere a disposizione una funzionalità che consenta ai destinatari dei loro servizi di dichiarare, oltre quanto indicato *supra* nella nota 15: «(e) [...] che non forniscono contenuti generati da sistemi di intelligenza artificiale senza sottoporre tali contenuti al riesame umano e al controllo editoriale; (f) [...] la ragione sociale e i dati di contatto [...]; e (g) [...] i dati di contatto delle autorità o degli organismi nazionali di regolamentazione competenti o dei rappresentanti dei meccanismi di coregolamentazione o di autoregolamentazione [...]».

nulla l'esenzione prevista da questo stesso Regolamento per i MSP. Infatti, a fronte di limitazioni indebite dei contenuti di un MSP da parte di una piattaforma online, le procedure *ex post* previste dall'art. 18 dell'EMFA¹⁷ non sarebbero sufficienti a garantire il rispetto della libertà editoriale dei MSP, considerata la natura delle informazioni che sono soggette ad una rapida obsolescenza¹⁸.

La soluzione a tale questione dovrebbe consistere in un'interpretazione restrittiva delle regole che derogano al *media privilege*, anche mediante il coordinamento delle norme in campo.

Pertanto, se le deroghe non fossero interpretate ed applicate in modo restrittivo e i MSP fossero esposti a condotte discrezionali dei VLOPP in esito ad un sistema interno di autoregolamentazione consentito dallo stesso DSA, potrebbero porsi dubbi di legittimità dell'EMFA e del DSA, data la natura ampia e incerta dei criteri applicabili alle attività

dei VLOPP ai sensi di tali regolamenti europei e visto il "ruolo unico" riconosciuto ai MSP.

Inoltre, sempre in ragione di tale ruolo unico dei MSP, sui VLOPP dovrebbe gravare una speciale responsabilità nello svolgimento delle loro attività nei confronti di tali soggetti in applicazione degli artt. 28, 34 e 35 del DSA e dell'art. 28 *ter* della Direttiva SMA¹⁹, nonché più in generale in esecuzione dei loro obblighi, ai sensi del diritto dell'Unione, rispetto ai presunti contenuti illegali diffusi attraverso MS. In questo senso, ci si potrebbe chiedere se gli obblighi di buona fede e diligenza a carico dei VLOPP²⁰ possano richiedere la predisposizione, da parte degli stessi, di procedure che implicino verifiche e attività di coordinamento con le pertinenti Autorità e gli organismi di autoregolamentazione e coregolamentazione dei MS o comunque precisazioni in merito al loro campo di azione, al fine di ridurre i rischi di possibili impatti negativi delle loro decisioni sulla libertà dei MS²¹.

17. V. parr. 5 (obbligo di gestione prioritaria e senza indebito ritardo dei reclami dei MSP), 6 (obbligo di avviare dialogo significativo ed efficace con il fornitore di servizi di media, dietro sua richiesta), 7 (mediazione e risoluzione extragiudiziale delle controversie).

18. CERRINA FERONI 2024 osserva che «nel mondo dell'informazione il fattore temporale è essenziale in quanto una notizia che ha valore oggi potrebbe non averne più alcuno l'indomani», come riconosciuto dalla Corte EDU: «le notizie sono un bene deperibile e ritardarne la pubblicazione, anche per un breve periodo, può privarle di tutto il loro valore e interesse» (*Observer e Guardian c. Regno Unito*, ric. n. 13585/88, 26 novembre 1991, § 60).

19. Direttiva (UE) 2018/1808 del 14 novembre 2018 recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato (in questo contributo, definita anche "Direttiva SMA").

20. Considerando 2, 26, 40, 41, 76, 86, 103, 109 e artt. 14 e 34 del DSA.

21. V. il considerando 50 dell'EMFA che sottolinea l'importanza di tenere conto della libertà e del pluralismo dei media, in linea con il DSA, qualora il VLOPP ritenga che i contenuti forniti da un MSP siano incompatibili con i suoi termini e condizioni. V. anche considerando 86 del DSA sull'obbligo dei VLOPP di rispettare i diritti fondamentali quando adottano le misure necessarie per attenuare i rischi sistemici. Tali misure «dovrebbero essere proporzionate [...], tenendo debitamente conto dei potenziali effetti negativi su tali diritti fondamentali. Tali fornitori dovrebbero prestare particolare attenzione all'impatto sulla libertà di espressione». Per completezza, si osserva che il testo dell'art. 18 dell'EMFA non reca l'emendamento proposto dal Parlamento europeo, e cioè la previsione secondo cui se dopo l'interlocuzione con il MS il VLOPP ritiene «che il servizio di media [...] sia incompatibile con i propri termini e condizioni, può deferire il caso alla pertinente autorità o al pertinente organismo nazionale di regolamentazione competente o all'organismo del meccanismo di autoregolamentazione o di coregolamentazione interessato» (v. Emendamenti del Parlamento europeo, approvati il 3 ottobre 2023, OJ C, C/2024/1196, 23 febbraio 2024). ERGA (*European Regulators Group for Audiovisual Media Services*) osserva, da un lato, che richiedere alle Autorità nazionali di valutare le condizioni generali delle VLOPP potrebbe eccedere il loro mandato; dall'altro, accoglie positivamente «the involvement of the NRAs for the protection of media service providers from unjustified content moderation decisions by platforms [...]» (v. ERGA recommendations for EMFA trilogues (October 2023), nel commento all'art. 17, lett. H)).

Un approccio interpretativo diverso rischierebbe non solo di compromettere diritti fondamentali della Carta, ma anche di trasferire a soggetti privati competenze e poteri che, con riguardo ai MSP, dovrebbero tendenzialmente rimanere in capo alle Autorità nazionali di regolamentazione e agli organismi nazionali di autoregolamentazione e coregolamentazione.

Le competenze di tali Autorità ed organismi dovrebbero invece essere rafforzate, anziché indebolite, in particolare mediante l'adeguamento dei loro poteri di vigilanza e sanzionatori all'ambiente online, nel rispetto dei diritti fondamentali.

Inoltre, ogni intervento del Consiglio europeo per i servizi mediatici (il "Consiglio"), del Comitato di contatto ("Comitato") e della Commissione europea, ai sensi dell'EMFA²², diretto a circoscrivere la discrezionalità dei VLOPP nell'applicazione della deroga di cui all'art. 18, par. 4, ult. co., sarebbe fortemente auspicabile potendo contribuire alla certezza del diritto «necessaria per beneficiare dei vantaggi di un mercato integrato e sviluppato»²³.

Né qui soccorrerebbe il considerando 75 del DSA che prevede che gli «obblighi supplementari per i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi sono necessari per affrontare [tali] preoccupazioni di interesse pubblico, in quanto non esistono misure alternative e

meno restrittive che consentano di conseguire efficacemente lo stesso risultato».

Infatti, nel bilanciamento tra i potenziali rischi derivanti dalla circolazione online delle informazioni fornite da MSP e la protezione della libertà e del pluralismo dei MSP, quest'ultima dovrebbe prevalere, visti anche i requisiti richiesti per l'accesso al beneficio del *media privilege*²⁴ e considerate le garanzie che, quantomeno astrattamente, dovrebbero sempre assistere l'attività di moderazione delle piattaforme online con riguardo al rispetto dei diritti fondamentali²⁵.

Ciò è tantopiù vero quando tali diritti riguardano MSP "qualificati" ai sensi dell'EMFA, e cioè a dire destinatari dei servizi online che sono già tenuti al rispetto di «standard di credibilità e trasparenza»²⁶, che sono soggetti a potestà regolamentari nei singoli Stati membri e che, rispetto ad ogni altro soggetto, sono preventivamente conoscibili dai VLOPP grazie al sistema delle dichiarazioni contemplate dal primo par. dell'art. 18 dell'EMFA²⁷.

Lo scopo di questa analisi è di fornire alcune riflessioni che potrebbero essere utili a meglio individuare il campo di azione dei VLOPP nei riguardi dei MSP qualificati, anche alla luce delle migliori pratiche²⁸, e tenuto conto dell'esigenza di salvaguardare i diritti fondamentali di questi ultimi.

22. Considerando 41, 45, 46, 53, 55, 56. artt. 13, 16, 18, 19 dell'EMFA.

23. Considerando 14 dell'EMFA.

24. V. *supra* nota 15.

25. Artt. 14 par. 4, 17, 20 par. 1, 21, 23, 53 del DSA. Sugli obblighi applicabili ai VLOPP, si osserva che «Overall, the guidance provided in the DSA as regards the application and enforcement of these provisions in connection with Article 14 is limited and significant uncertainty remains. It is possible to identify a number of challenges. First, at a minimum, Articles 17 and 20 mean that [...] VLOPs will have to not only offer clarity on the contractual or legal basis for the decision but also on whether the enforcement of these norms is in line with the applicable fundamental rights. Yet, given the enormous amount of content reviewed by platforms, the level of detail and nuance in these individual cases required for compliance remains to be seen. Second, and similarly, the lack of guidance in Article 14(4) DSA itself on how the weighing of the different interests and rights that should be involved, adds another layer of uncertainty as to whether it will, in practice, work [...]» (così QUINTAIS-APPELMAN-FATHAIGH 2023, p. 905). V. anche PAPA-EVANGELOU 2023, p. 469. Il tema verrà ripreso al successivo paragrafo 2.2.

26. Considerando 55 dell'EMFA.

27. Si ricorda che gli operatori commerciali sono identificabili (Sezione 4 del DSA, in particolare art. 30), ma non rilevanti in questo contesto.

28. Ai fini di questo contributo, il riferimento è alla prassi delle piattaforme televisive.

2. Gli obiettivi dell'EMFA e il suo art. 18

Dopo aver sottolineato che nel mercato interno dei MS, sempre più digitale e internazionale, è essenziale preservare il “ruolo unico” di tali servizi tutelandone la libertà e il pluralismo quali due dei pilastri principali della democrazia e dello stato di diritto²⁹, l'EMFA dispone:

- a) il diritto dei destinatari dei MS di «avere accesso a una pluralità di contenuti mediatici editorialmente indipendenti»³⁰;
- b) il diritto dei MSP di «esercitare le loro attività economiche nel mercato interno senza restrizioni che non siano quelle consentite a norma del diritto dell'Unione»³¹ e
- c) l'obbligo degli Stati membri, comprese le autorità e gli organismi nazionali di regolamentazione, di non interferire «con le politiche e le decisioni editoriali dei fornitori di servizi di media» e di non influenzarle³².

Nel nuovo ecosistema digitale, le VLOP rappresentano «punti di accesso ai contenuti e ai servizi di media per molti utenti»³³.

Ai sensi dell'EMFA, qualora un VLOPP dovesse considerare incompatibili con le proprie condizioni generali uno o più dei contenuti di tali servizi, gli stessi dovrebbero «tenere debitamente conto della libertà e del pluralismo dei media [...] e fornire il prima possibile le necessarie spiegazioni ai fornitori di servizi di media esponendo le motivazioni alla base delle loro decisioni [...]. [...] prima

che la sospensione o la limitazione della visibilità abbiano effetto. Inoltre, dovrebbero dare al fornitore di servizi di media la possibilità di rispondere alla motivazione [...]»³⁴.

È, come si è visto, il cosiddetto *media privilege* da non confondere con le garanzie che le piattaforme online devono comunque osservare nei rapporti con i destinatari dei loro servizi³⁵. Il *media privilege* rappresenta, infatti, una garanzia in qualche modo aggiuntiva a favore di soggetti che, come visto, rivestono un “ruolo unico” in un sistema democratico.

Si noti che il *media privilege* sembra riguardare solo i contenuti che siano considerati dal VLOPP in contrasto con le condizioni generali di utilizzo del suo servizio, mentre esso non viene riferito anche ai “contenuti illegali” (quest'ultimo termine ricorre invece nel DSA pressoché sempre, quando si citano le condizioni generali dei VLOPP)³⁶.

Questo implica che il *media privilege* non dovrebbe operare per i contenuti illegali a meno che questi ultimi siano richiamati nelle condizioni generali del VLOPP e sempre che non si applichi per questi contenuti – come appare ragionevole ritenere anche sulla base della lettura coordinata con le norme del DSA – il solo par. 4, ult. co. dell'art. 18 dell'EMFA per i casi in cui il VLOPP sia tenuto, con riguardo a tali contenuti, a conformarsi a taluni obblighi³⁷.

29. Considerando 2.

30. Art. 3.

31. Art. 4, parr. 1 e 2.

32. *Ibidem*.

33. Considerando 50. Sui diversi tipi di VLOP v. BROUGHTON MICOVA-SCHNURR-CALEF-ENSTONE 2024, p. 17.

34. Considerando 50.

35. Artt. 20, 21, 23 e 24 del DSA.

36. Infatti, l'EMFA non si riferisce ai contenuti “illegali” per la temporanea limitazione delle procedure di sospensione o di limitazione della visibilità dei contenuti, ma solo alle condizioni generali di contratto del VLOPP. Invece, il DSA indica quali cause di possibile rimozione di, o di disabilitazione dell'accesso a, informazioni i contenuti che sono illegali o che sono incompatibili con le condizioni generali. V. considerando 54, 58, 64, 80, 84 e artt. 3, par. 1, lett. t (che, nella nozione di “moderazione dei contenuti”, include i “contenuti illegali” e le “informazioni incompatibili con le condizioni generali”), 15, par. 1, lett. c), 17, 20, parr. 1 e 4, 34, par. 2, 39, par. 3. Come rilevato, i contenuti illegali sono espressamente previsti nell'EMFA all'art. 18, par. 4, ult. co. dove si menzionano gli “obblighi relativi ai contenuti illegali che incombono loro in forza del diritto dell'Unione”. Per altri riff. ai contenuti illegali, v. *infra* nota 162.

37. Artt. 9, 10, 16 e 22 del DSA (ordini di contrastare i contenuti illegali e di fornire informazioni, il meccanismo di segnalazione e azione, nonché i segnalatori attendibili di contenuti illegali). Vi sono anche gli obblighi sui

Pertanto, seguendo tale lettura delle norme, il *media privilege*, sarebbe applicabile ai soli contenuti in contrasto con le condizioni generali del suo servizio, inclusi i contenuti che il VLOPP valutasse come anche solo dannosi³⁸ nell'ambito delle sue attività³⁹ e in particolare nello svolgimento di quelle di moderazione⁴⁰ e ferma restando la sua inapplicabilità nel caso in cui il VLOPP fosse tenuto ad ottemperare a suoi obblighi conformemente al diritto dell'Unione.

Infatti, come visto, l'EMFA precisa che nulla di quanto previsto nello stesso può essere interpretato come una deroga agli obblighi dei VLOPP ai sensi degli artt. 28 (tutela minori), 34 (rischi sistemici) e 35 (misure di attenuazione) del DSA e dell'art. 28 *ter* della direttiva 2010/13/UE⁴¹⁻⁴².

Più precisamente, nel testo dell'art. 18, par. 4, ult. co., il legislatore unionale si esprime in termini

di "inapplicabilità" del *media privilege* nel caso di sospensione della fornitura dei propri servizi in relazione a contenuti forniti da un MSP o di limitazione della visibilità di tali contenuti conformemente ai loro obblighi a norma degli artt. 28, 34 e 35 del DSA e dell'articolo 28 *ter* della Direttiva SMA o conformemente agli obblighi a carico dei VLOPP ai sensi del diritto dell'Unione relativamente ai contenuti illegali.

In sintesi, la norma in esame stabilisce che, in tali casi, la procedura relativa al *media privilege* non opera⁴³, mentre rimangono fermi tutti i successivi paragrafi dell'art. 18 dell'EMFA⁴⁴. Non è dunque un tema di applicazione di obblighi che "corrono in parallelo", e cioè quelli sul *media privilege* e quelli di cui ai menzionati articoli del DSA e della Direttiva SMA, bensì di totale inapplicabilità ai MS del primo al ricorrere dei casi previsti in tali articoli.

contenuti illegali previsti in altri atti unionali, come la Direttiva DSM (v. *infra* nota 87), il Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio del 29 aprile 2021 relativo al contrasto della diffusione di contenuti terroristici online.

38. Mentre per i "contenuti illegali" viene fornita, all'art. 3, par. 1, lett. h) del DSA, una definizione, non ne ve ne è una per i "contenuti dannosi", e cioè per i contenuti che, pur potendo essere legali, sono in grado di produrre effetti negativi sugli individui e sulla società, come ad es. la disinformazione. In merito a tale lacuna e ai relativi rischi, v. CANTERO GAMITO 2022, p. 10. Sui dubbi interpretativi che si pongono anche per la nozione di "contenuti illegali", v.: la Raccomandazione 2023/2425 del 20 ottobre 2023, adottata in vista della piena applicabilità del DSA, che rileva come tale Regolamento «non determina se un particolare tipo di contenuto possa qualificarsi come illegale. L'illiceità dei contenuti è determinata dalle leggi nazionali o, se armonizzate, dalle norme europee.» (considerando 11) ed elenca alcuni atti europei più specifici (v. *infra* nota 54); i considerando 16-17 del DSA sui protocolli di crisi; la Raccomandazione C(2023) 7170 final (considerando 15). V. anche quanto osserva HUSOVEC 2024, p. 49 ss.

39. Il *media privilege* non si estende ai motori di ricerca. Infatti, l'art. 18 riguarda solo le VLOP. V. posizione espressa da ERGA alla Commissione UE (v. *infra* nota 153).

40. Sulla definizione di «moderazione dei contenuti» v. art. 3, par. 1, lett. t) del DSA. Sulle attività di moderazione e l'EMFA si osserva che «This fundamentally changes content moderation practices vis-à-vis the media, which previously operated on a "remove and notify" basis. In some cases, such notifications were even missing or were overly general to be informative. Additionally, visibility reductions often lacked any individual notifications. This should no longer be the case for media once EMFA goes into full implementation [...]» (così NENADIC-BROGI 2024). Sulla moderazione, v. anche FOLKERT-KALÉDA-LOWENTHAL 2024, pp. 46 e 122 ss., TOURKOCHORITI 2023, p. 135 ss.

41. Si noti che l'art. 28 *ter* della Direttiva SMA non riguarda i VLOPP *tout court*, bensì i fornitori di servizi di piattaforma per la condivisione di video, come definiti all'art. 1, par. 1, lett. a *bis* e d *bis* di quest'ultima Direttiva. Si tratta di fornitori di piattaforme on line che rappresentano una *species* del più ampio *genus* delle piattaforme online di cui al DSA (art. 3, par. 1, lett. i)) e che sono state, al contempo, designate come VLOP ai sensi del DSA. V. meglio *infra* paragrafo 5.2.

42. Considerando 51.

43. Il riferimento è al "presente paragrafo", e cioè al par. 4 dell'art. 18 che precede il suo ult. co.

44. V. *infra* paragrafo 2.1.

La lettera della norma è chiara a prima vista, ma come vedremo, pone rilevanti questioni, in particolare per quanto riguarda la tutela effettiva dei diritti fondamentali, con specifico riferimento alla libertà dei MSP e al loro pluralismo, a causa della discrezionalità di cui i VLOPP godono nell'applicazione delle suddette norme. Inoltre, per l'art. 28 *ter* della Direttiva SMA, sussiste anche un tema di possibile inapplicabilità dello stesso ai SMA, per le ragioni che saranno illustrate⁴⁵.

2.1. La procedura *ex ante* e *ex post* del *media privilege*

La procedura relativa al *media privilege* viene descritta all'art. 18, par. 4 dell'EMFA ed essa presuppone, come già indicato, una previa qualificazione del MSP ai sensi dell'art. 18, par. 1, dovendo quest'ultimo possedere una serie di requisiti (MSP che risponde a tali requisiti, per brevità viene indicato con il termine "MSP qualificato/i")⁴⁶.

La qualificazione riguarda il soggetto e non l'oggetto, ovvero riguarda lo "*status*" del MSP e non dei suoi prodotti editoriali. Questo aspetto ha una sua rilevanza, come verrà meglio chiarito di seguito.

La procedura prevede che (*ex ante*) il MSP qualificato disponga di 24 ore per rispondere alla notifica del VLOPP con la quale questi gli comunica che il contenuto presente sulla piattaforma è incompatibile con i suoi termini e condizioni⁴⁷ e, nei casi di "crisi"⁴⁸, entro un termine più breve che

conceda al MSP tempo sufficiente per rispondere «in modo significativo»⁴⁹.

Qualora, ciononostante, il VLOPP decida di sospendere o limitare la visibilità del contenuto contestato, ne informa senza indebito ritardo il MSP che potrà avvalersi (*ex post*) dei seguenti "rimedi" previsti ai parr. 6 e 7 dell'art. 18:

- 1) su sua richiesta, il VLOPP dovrà avviare un dialogo per individuare una soluzione amichevole che ponga fine a limitazioni o sospensioni "ingiustificate" e ad evitare che ve ne siano altre in futuro;
 - 2) comunicare gli esiti del dialogo al Comitato di contatto⁵⁰ e alla Commissione europea;
 - 3) chiedere al Comitato di emettere un parere sull'esito del dialogo, compresa l'indicazione di azioni raccomandate per il VLOPP;
 - 4) ricorrere alla mediazione di cui all'art. 12 del Regolamento (UE) 2019/1150 o alla risoluzione extragiudiziale delle controversie di cui all'art. 21 del DSA.
- Inoltre:
- 5) viene garantita la trasparenza del VLOPP in merito all'applicazione dell'art. 18 del DSA, essendo tenuto a rendere disponibili al pubblico, su base annuale, un report delle sue attività⁵¹;
 - 6) la Commissione pubblica orientamenti con particolare riferimento all'attuazione della funzionalità richiesta al VLOPP per la dichiarazione necessaria agli MSP per essere "qualificati"⁵²;

45. V. *infra* paragrafo 5.5.

46. V. *supra* nota 15.

47. Art. 18, par. 4, co. 1, dell'EMFA.

48. La norma disciplina le situazioni di crisi (considerando 91 e art. 36, par. 2, co. 1 del DSA).

49. Art. 35, par. 4, co. 1, lett. b).

50. Si tratta del Comitato Europeo per i Servizi di Media (EMBS – *European Board for Media Services*) che sarà operativo dall'8 febbraio 2025 (art. 8 dell'EMFA). Tale Comitato non va confuso con lo *European Board for Digital Services*, previsto dal DSA, che è invece composto dai Coordinatori dei servizi digitali. «Both Boards formally have an independent advisory role, but their guidelines and recommendations will, in fact, be crucial for adequate and harmonised enforcement of the two new pieces of EU law, especially on complex, sensitive, and intersecting issues». (così NENADIC–BROGI 2024).

51. Art. 18, par. 8. NENADIC–BROGI 2024, osservano che «regular and informed monitoring of how platforms implement systemic risk assessment and mitigation [...] is crucial. This area concerns fundamental rights, and the way these rights and systemic risks are operationalised under the DSA will determine the potential of both the DSA and the EMFA to safeguard media freedom in platforms' content moderation». Sugli obblighi di monitoraggio, v. anche GOSZTONYI–GALEWSKA–ŠKOLKAY 2024.

52. Art. 18, par. 9, dell'EMFA.

- 7) il Comitato organizza regolarmente un dialogo strutturato tra i soggetti interessati (VLOPP, rappresentanti dei MSP e della società civile) e fornisce i relativi risultati alla Commissione⁵³

Alla luce di tali norme, emergono immediatamente le seguenti considerazioni.

La disciplina del beneficio del *media privilege* appare, nel complesso, piuttosto fragile poiché, anche quando è applicabile, la verifica della conformità dei contenuti dei MS qualificati si concentra sul rispetto delle condizioni generali dei VLOPP, senza un esplicito riferimento alle prescrizioni normative, incluse quelle di regolamentazione, coregolamentazione o autoregolamentazione menzionate nel primo paragrafo dell'art. 18, lett. d). Queste norme dovrebbero essere considerate come parametri di riferimento per l'applicazione delle condizioni generali ai fini della sospensione o limitazione della visibilità di un contenuto di un MSP qualificato. Inoltre, le tempistiche per la gestione del contraddittorio sono piuttosto ristrette, non consentendo il pieno esercizio dei diritti di difesa da parte di un MSP qualificato di fronte a una contestazione infondata.

Con riguardo al primo aspetto, emerge subito un dato.

Infatti, l'EMFA sembra differenziarsi dal Regolamento europeo, adottato solo un anno e mezzo prima, con riguardo alla diffusione online di

contenuti terroristici che appare maggiormente tutelante per i MS⁵⁴.

Quest'ultimo Regolamento precisa che «In particolare nei casi in cui il fornitore di contenuti detenga una responsabilità editoriale, qualsiasi decisione relativa alla rimozione del materiale diffuso dovrebbe tenere conto delle norme giornalistiche previste dalla regolamentazione della stampa o dei media in conformità al diritto dell'Unione, compresa la Carta. Inoltre, le opinioni radicali, polemiche o controverse espresse nell'ambito di dibattiti politici sensibili non dovrebbero essere considerate contenuti terroristici.»⁵⁵.

A questo riguardo potrebbe soccorrere l'orientamento consolidato della Corte di Giustizia che riconosce che «l'interpretazione di una disposizione del diritto dell'Unione richiede di tener conto non soltanto della sua formulazione, ma anche del contesto in cui essa si inserisce nonché degli obiettivi e della finalità che persegue l'atto di cui essa fa parte»⁵⁶.

Infatti, mal si giustificerebbe un approccio differenziato nei confronti dei MSP, ai sensi dell'EMFA e del DSA, da un lato, e del Regolamento europeo sul contrasto della diffusione online di contenuti terroristici, dall'altro lato, tantopiù che la tutela rispetto alla diffusione online di contenuti terroristici rappresenta un ambito di elevata criticità⁵⁷ e, pertanto, di riferimento anche per altri tipi di contenuto⁵⁸.

53. Tale dialogo ha la finalità di: a) discutere delle esperienze e delle migliori pratiche relativamente all'applicazione dell'articolo 18, anche per quanto riguarda i processi di moderazione dei contenuti dei MSP; b) promuovere l'accesso a offerte diversificate di media indipendenti su piattaforme online di dimensioni molto grandi; e c) monitorare l'adesione alle iniziative di autoregolamentazione volte a proteggere gli utenti da contenuti nocivi, incluse le ingerenze da parte di attori stranieri.

54. Sul Regolamento europeo sul contrasto della diffusione di contenuti terroristici online BARATA 2021 osserva però che: «The Regulation incorporates imprecise guidelines establishing that when adopting such measures providers need to take into account “the risks and level of exposure to terrorist content as well as the effects on the rights of third parties and the public interest to information” (recital 22). Designated “competent authorities” (*sic*) will “determine whether the measures are effective and proportionate”.» (p. 11).

55. Considerando 12 del Regolamento europeo sul contrasto della diffusione di contenuti terroristici online.

56. Sentenza C-566/22, 8 febbraio 2024, § 15; sentenza C579/21, 22 giugno 2023, § 38 e giurisprudenza ivi citata; sentenza C-634/21, 7 dicembre 2023, § 41.

57. Sulla nozione di «contenuti terroristici», v. il considerando 11 del Regolamento europeo sul contrasto della diffusione online di contenuti terroristici: «tale definizione dovrebbe ricomprendere il materiale che istiga o sollecita a commettere o a contribuire alla commissione di reati di terrorismo, o sollecita a partecipare alle attività di un gruppo terroristico o fa l'apologia di attività terroristiche, incluse raffigurazioni di un attentato terroristico [...]».

58. Il Regolamento europeo sul contrasto della diffusione online di contenuti terroristici prevede, più in generale, che «In caso di conflitto tra il presente regolamento e la direttiva 2010/13/UE [...] per quanto riguarda le disposizioni che disciplinano i servizi di media audiovisivi [...], la direttiva [...] dovrebbe prevalere. Ciò lascia

Seguendo questo approccio, poiché l'EMFA mira a rafforzare l'indipendenza e il pluralismo dei MS e, a tal fine, interviene sulle procedure dei VLOPP relative alla rimozione o limitazione dei contenuti dei MS, si dovrebbe ritenere che, nelle loro attività di moderazione, i VLOPP debbano considerare – quale necessario parametro di riferimento – gli standard regolamentari applicabili ai MSP qualificati⁵⁹.

A tale conclusione si giunge anche sulla base delle successive disposizioni dell'art. 18 dell'EMFA che evidenziano quanto il *media privilege* sia soggetto a valutazioni discrezionali da parte dei VLOPP e quanto sia dunque necessario che questi ultimi dispongano di punti di riferimento certi per le loro valutazioni, come gli standard regolamentari applicabili ai MSP nel loro Stato membro di appartenenza.

Così ad esempio, il successivo eventuale dialogo tra il VLOPP e il MSP, previsto all'art. 18, par. 6, dell'EMFA, è strumentale a porre fine a limitazioni o sospensioni “ingiustificate” e ad evitare che ve ne siano altre “in futuro” (v. anche sopra punto i)). Tale circostanza evidenzia come, almeno sulla “carta”, venga accettato il rischio che le limitazioni o sospensioni dei contenuti dei MSP qualificati, da

parte dei VLOPP, possano essere ingiustificate. In tale dialogo, peraltro, i MSP saranno naturalmente portati a richiamare la regolamentazione agli stessi applicabile e a indicare le Autorità ed organismi di riferimento per la corretta valutazione delle loro condotte.

Non si vede dunque la ragione per cui tali standard regolamentari non debbano essere il necessario parametro di riferimento per i VLOPP nella valutazione *ex ante* dei contenuti dei MSP⁶⁰.

Infatti, come sottolineato, i soli rimedi *ex post* non risultano sufficienti a garantire il pieno rispetto della libertà editoriale dei MSP, dal momento che i contenuti eventualmente oggetto di ripristino potrebbero aver perso nel frattempo di interesse per il pubblico⁶¹, nonché in considerazione del fatto che i MSP potrebbero essere portati a conformare spontaneamente la propria linea editoriale alle prescrizioni dei VLOPP anche al fine di evitare conseguenze più gravi come la chiusura del proprio account (cd. *chilling effect*)⁶².

Pertanto, un mero approccio *ex post*, quale “sede” per una verifica degli standard regolamentari applicabili al MSP oggetto di eventuali restrizioni da parte di un VLOPP, non è idoneo, ad avviso di chi scrive, a superare il probabile *vulnus* al diritto

impregiudicati gli obblighi di cui al presente regolamento, in particolare per quanto riguarda i fornitori di servizi di piattaforma per la condivisione di video». (considerando 8). Pertanto, la specialità del diritto applicabile quantomeno ai SMA viene ribadita a dimostrazione della specifica tutela della libertà e indipendenza dei SMA. In tal senso v. anche i considerando 1, 10, 12, 23, 49 del suddetto Regolamento.

59. L'art. 14 del DSA, sui “Termini e Condizioni” dei prestatori di servizi intermediari, prevede l'obbligo di agire in modo diligente, obiettivo e proporzionato nell'applicare e far rispettare tali termini e condizioni «tenendo debitamente conto dei diritti e degli interessi legittimi di tutte le parti coinvolte, compresi i diritti fondamentali dei destinatari del servizio, quali la libertà di espressione, la libertà e il pluralismo dei media, [...]». Sulle obbligazioni di diligenza contenute nel Capitolo III del DSA applicabili, in diversa misura, ai fornitori di servizi intermediari, a seconda che si tratti di figure “base” (*mere conduit*, *caching* o *hosting provider*), di piattaforme online o di piattaforme online (o motori di ricerca) di dimensioni molto grandi e sulle obbligazioni speciali (artt. 33-43 del DSA) applicabili a queste ultime piattaforme, v. anche DEL MORAL SÁNCHEZ 2024, p. 15 ss.; DERGACHEVA–KUZNETSOVA–SCHARLACH–KATZENBACH 2023; MONTI 2019.

60. Qui non viene affrontato il tema collegato della delega ai VLOPP di poteri assimilabili a quelli regolamentari – che verrà trattato al successivo paragrafo 2.2.

61. V. *supra* nota 18.

62. L'EMFA si esprime in termini di «sospensione della fornitura dei propri servizi di intermediazione online relativi ai contenuti forniti dal fornitore di servizi di media o alla limitazione della visibilità di tali contenuti» e risulta dunque includere anche la chiusura dell'account. ERGA aveva rilevato l'utilità di chiarimenti a riguardo (“*Proposal of the Commission for a European Media Freedom Act (EMFA). Erga position*”), November 2022, nel commento gli artt. 17-18 della Proposta di DSA, lett. GG). In merito al c.d. “chilling effect”, v. QUINTAIS–APPEL–MAN–FATHAIGH 2023, p. 886, nonché la giurisprudenza della Corte EDU e la dottrina ivi richiamate.

fondamentale ad una pluralità di contenuti mediatici editorialmente indipendenti.

2.2. I diritti fondamentali dei fornitori di servizi di media

In base al nuovo assetto normativo introdotto dal DSA⁶³, i VLOPP, nel progettare, applicare e far rispettare le restrizioni imposte da quest'ultimo Regolamento, devono tener conto dei diritti fondamentali sanciti dalla Carta. Pertanto, le loro attività devono essere organizzate in modo da garantire l'effettiva tutela di tali diritti.

I diritti fondamentali dei MSP trovano il proprio riconoscimento iniziale nella Convenzione Europea dei Diritti dell'Uomo («CEDU»)⁶⁴.

Infatti, anche se l'art. 10⁶⁵ della CEDU tutela la libertà di espressione senza un esplicito

riferimento ai media⁶⁶, la giurisprudenza consolidata della Corte di Strasburgo⁶⁷ riconosce il ruolo fondamentale di questi ultimi, in particolare dei Servizi di Media Audiovisivi (SMA), nell'esplicazione della libertà di espressione in una società democratica⁶⁸.

Con la Carta, la libertà e il pluralismo dei media vengono espressamente codificati, sancendo che: «La libertà dei media e il loro pluralismo sono rispettati» (art. 11)⁶⁹.

La Corte di Giustizia ha riconosciuto che «la salvaguardia delle libertà protette dall'articolo 11 della Carta dei diritti fondamentali, tra le quali figurano, al paragrafo 2, la libertà e il pluralismo dei media, costituisce incontestabilmente un obiettivo di interesse generale, di cui occorre sottolineare, in

63. Sul DSA, v. anche DEL MORAL SÁNCHEZ 2024, FOLKERT-KALÈDA-LOWENTHAL 2024; CHIARELLA 2023, pp. 33-58; CHURCH 2023, pp. 53-59, CHIRICO 2023, p. 45 ss.; BOLOGNINI-PELINO-SCIALDONE 2023, pp. 3-235; MARTINELLI 2023, p. 107 ss.; VAN HOBOKEN-QUINTAIS-APPELMAN-FAHY et al. 2023; SCHLAG 2023, pp. 168-177; TOURKOCHORITI 2023; BURI-VAN HOBOKEN 2022; GOANTA-BERTAGLIA-IAMNITCHI 2022; CAGGIANO 2021; COLE-ETTELDOERF-ULLRICH 2021; RODRÍGUEZ DE LAS HERAS BALLELL 2021.

64. Poiché l'adesione dell'Unione alla CEDU non è stata perfezionata, essa «non vincola direttamente l'Unione anche se il suo contenuto contribuisce a formare i principi generali [...]», DANIELE 2020, p. 201.

65. V. primo co. dell'art. 10 (Libertà di espressione): «Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera [...]».

66. Sulla CEDU come «fonte di ispirazione» per l'elaborazione dei principi generali del diritto dell'Unione europea, v. PSYCHOGIOPOULOU 2022. Secondo la Corte di Giustizia, «i diritti fondamentali fanno parte integrante dei principi generali del diritto, dei quali la Corte garantisce l'osservanza. [...] La Convenzione europea dei diritti dell'uomo riveste, a questo proposito, un particolare significato [...]» (sentenza C-260/89, 18 giugno 1991, §41). V. anche LO TAURO 2016, p. 51 ss.; McMILLAN 2019, nonché sentenze della Corte di Giustizia, C-29/69, 12 novembre 1969; C-11/70, 17 dicembre 1970; C-4/73, 14 maggio 1974.

67. La Corte Europea dei Diritti dell'Uomo (Corte EDU), con sede a Strasburgo, è l'organo giurisdizionale competente a giudicare «tutte le questioni riguardanti l'interpretazione e l'applicazione della Convenzione e dei suoi Protocolli» (art. 32 della CEDU).

68. La Corte EDU ha ribadito che «Non vi è democrazia senza pluralismo» e che «I media audiovisivi hanno un ruolo particolarmente importante da svolgere a tale riguardo. A causa del loro potere di far passare dei messaggi attraverso il suono e l'immagine, hanno effetti più immediati e più potenti della stampa scritta» (*Associazione politica nazionale lista Marco Pannella e radicali italiani c. Italia*, 30 novembre 2021, ricorso n. 20002/13, §79, §81). V. anche causa *Jersild c. Danimarca*, 23 settembre 1994, §31, serie A n. 298; causa *Centro Europa 7 s.r.l. e Di Stefano c. Italia*, 7 giugno 2012, ricorso n. 38433/09, §129, §132.

69. V. anche considerando 3 della Raccomandazione (UE) 2022/1634 sulle garanzie interne di indipendenza editoriale e la trasparenza della proprietà nel settore dei media («I fornitori di servizi di media usufruiscono [...] della protezione [...] loro garantita dall'articolo 11 della Carta. [...]»). Tale Raccomandazione affianca la proposta legislativa per un regolamento che istituisca un quadro comune per i servizi di media sul mercato interno (divenuto poi l'EMFA) «quale strumento di effetto immediato per promuovere l'indipendenza editoriale e la trasparenza della proprietà dei media [...]» (considerando 6).

particolare, l'importanza in una società democratica e pluralista [...]»⁷⁰⁻⁷¹.

Le disposizioni di cui all'art. 11 della Carta si applicano alle istituzioni e organi dell'Unione e degli Stati membri quando attuano il diritto dell'Unione (art. 51, co. 1, della Carta)⁷².

La questione dell'efficacia diretta della Carta nei rapporti tra privati ha suscitato un ampio dibattito. In questo contesto, si osserva che il Regolamento europeo sul contrasto alla diffusione di contenuti terroristici online e il DSA stabiliscono esplicitamente l'obbligo, anche per i privati (in particolare i VLOPP), di rispettare i diritti fondamentali tutelati dalla Carta, con particolare riferimento a quelli di cui all'art. 11⁷³.

Infatti, entrambi i suddetti regolamenti europei prevedono il rispetto dei diritti fondamentali dei media, inclusi quelli di cui alla Carta, da parte delle piattaforme online⁷⁴. Per questo aspetto, tali regolamenti europei rispondono alle

istanze internazionali di garantire che le attività delle piattaforme online, in particolare le attività di moderazione, «siano guidate dagli stessi standard di legalità, necessità e legittimità che vincolano gli Stati nella regolamentazione della libertà di espressione»⁷⁵.

A tale riguardo, è rilevante quanto afferma il Comitato dei Ministri nella sua Raccomandazione 2018 e cioè che «Internet intermediaries should in all their actions respect the internationally recognised human rights and fundamental freedoms of their users and of other parties who are affected by their activities. This responsibility, in line with the United Nations Guiding Principles on Business and Human Rights, exists independently of the States' ability or willingness to fulfil their own human rights obligations»⁷⁶.

Pertanto, si potrebbe ritenere che, nella misura in cui un VLOPP dovesse violare la libertà dei media in sede di applicazione degli artt. 28, 34 o

70. Corte di Giustizia C-719/18, 3 settembre 2020, § 57.

71. L'art. 52, co. 3 della Carta dispone che, qualora essa faccia riferimento a diritti presenti nella CEDU, «questi vadano interpretati in maniera analoga a quelli convenzionali o, meglio, intendendo quelli convenzionali come *minimum standard*, con la conseguente possibilità di espansione delle libertà e dei diritti garantiti dalla CEDU». (MONTI 2020, pp. 285-286). V. anche sentenza della Corte di Giustizia che ha affermato che all'art. 11 della Carta occorre riconoscere lo stesso significato e obiettivo dell'art. 10 della CEDU, così come interpretato dalla Corte EDU (sentenza C-460/20, 8 dicembre 2022, § 59).

72. In merito alle critiche sugli effetti orizzontali della Carta si osserva che «La formulazione dell'art. 51 porterebbe a ritenere che i privati sono esclusi dall'applicabilità orizzontale perché i soggetti cui la norma (e dunque la Carta) si rivolge sono, da un lato le istituzioni, gli organi, gli organismi, dall'altro lato gli Stati che danno attuazione al diritto dell'Unione. La norma, tuttavia, non definisce l'ambito personale, bensì quello materiale: precisamente il perimetro di applicazione della Carta, nel rispetto delle competenze dell'Unione, che la Carta non può né modificare, né ampliare.» (così NASCIMBENE 2021, p. 89). Sugli effetti diretti della Carta lo stesso Autore sottolinea che «È riconosciuto effetto diretto alla Carta, ma in realtà lo è al principio generale che esisteva prima della Carta, [...]». La Corte riconosce che la mancata previsione, nell'art. 51, par. 1, Carta, dei soggetti privati fra i destinatari della Carta non esclude [...] che nelle situazioni giuridiche disciplinate dal diritto UE la Carta si applichi, in senso orizzontale, anche ai privati.» (ivi, p. 92). V. anche FERRARO 2019 e la giurisprudenza e dottrina richiamata.

73. Un richiamo espresso alla CEDU, e precisamente all'art. 10, viene fatto anche nella *Raccomandazione sulla libertà di internet* del 2016 (CM/Rec(2016)5) con riguardo ai principi di legalità, legittimità e proporzionalità da osservare nell'espletamento delle attività di blocco, filtraggio e rimozione dei contenuti (art. 2.1.6).

74. Con riferimento al Regolamento europeo sul contrasto della diffusione online di contenuti terroristici, v. in particolare considerando 9, 12, 20, 23 e art. 5.

75. V. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, United Nations, General Assembly, Human Rights Council Thirty-eighth session 18 June-6 July 2018 Agenda item 3 Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, punto 45.

76. Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the roles and responsibilities of internet intermediaries, § 2.1.1.

35 del DSA, potrebbe astrattamente porsi una questione di violazione, quantomeno indiretta, della Carta⁷⁷. In quest'ottica, è stato evidenziato che sia la CEDU sia la Carta potrebbero esplicitare effetti orizzontali, anche solo indiretti, nei confronti delle piattaforme online, ai sensi del DSA, applicando il criterio degli "obblighi positivi" a carico degli Stati membri⁷⁸. In base a questo approccio, non solo gli Stati aderenti a tali atti devono astenersi da condotte in violazione della libertà di espressione, ma devono porre in essere obblighi "positivi" per tutelarla anche nelle relazioni tra individui e imprese⁷⁹.

Infatti, la libertà di espressione deve essere protetta «persino nei confronti delle interferenze di soggetti privati»⁸⁰.

A tale riguardo, può essere utile ripercorrere i passaggi del DSA relativi al rispetto della Carta.

Il considerando 3 prevede che «Un comportamento responsabile e diligente da parte dei prestatori di servizi intermediari è essenziale per un ambiente online sicuro, prevedibile e affidabile e per consentire ai cittadini dell'Unione e ad altre persone di esercitare i loro diritti fondamentali garantiti dalla Carta dei diritti fondamentali

77. Si osserva che: «la Carta troverebbe applicazione in quanto la restrizione discenderebbe direttamente dall'adempimento ad un obbligo dettato dalla normativa europea.» (PALUMBO-PIEMONTE 2024, p. 120); «in terms of fundamental rights, individuals must be able to access courts when the obligations they benefit from have been violated, even without explicit remedies, as is mostly the case in the DMA and the DSA. This is a democratic imperative in the digital society according to the European Declaration on Digital Rights and Principles, and it is also part of the fundamental right to judicial protection under Article 47 of the Charter. Moreover, Article 19(2) of the TEU imposes the obligation of MS to "ensure effective legal protection" of EU law as a translation of the value of the Rule of Law enshrined in Article 2 TEU. However, not all their articles will be enforceable by private means. It will first depend on their clarity and preciseness and, second, on their objective of protecting the interests of a category of persons by conferring upon them rights correlative to the obligations incurred by digital firms» (DEL MORAL SÁNCHEZ 2024, p. 42); «however, there is no case law from the ECtHR or CJEU concerning a user initiating legal proceedings against a platform for removing content. Still, the important principles contained in the ECtHR judgments can be applied by platforms [...]» (QUINTAIS-APPELMAN-FATHAIGH 2023, p. 898); MANTELERO 2022.

78. V. art. 2.1.6. della *Raccomandazione sulla libertà di internet*, cit. Si sottolinea che «an important element of Article 10 ECHR and Article 11 Charter is the principle of positive obligations. Under the right to freedom of expression, States not only have a negative obligation to "abstain" from interfering with free expression, but they also have a positive obligation to protect free expression, "even in the sphere of relations between individuals," including between an individual and a "private company."» (QUINTAIS-APPELMAN-FATHAIGH 2023, p. 902). La Corte EDU è intervenuta con varie decisioni sulla nozione di "positive obligations" con riguardo al rispetto della libertà di espressione da parte di soggetti privati e ha fornito indicazioni sul bilanciamento dei diritti fondamentali (*Palomo Sánchez et al. v. Spain*, App. No. 28955/06, § 59 (Sept. 12, 2011); *Remusko v. Poland*, App. No. 1562/10, § 62 (July 16, 2013)). Le criticità sono state segnalate anche da FOLKERT-KALÉDA-LOWENTHAL 2024, p. 123 ss.; EDER 2024, p. 10 ss.; FROSIO-GEIGER 2023; EFRONI 2021; BARATA 2021; LAUX-WACHTER-MITTELSTADT 2021.

79. Sulla differenza tra "diretta applicabilità" ed "effetti diretti" del DSA, si osserva che «the case law of the Court establishes that provided that these conditions are fulfilled, regulations should enjoy both vertical, (in relations between the State and the individual) and horizontal, (in conflicts between individuals) effects» (v. DEL MORAL SÁNCHEZ 2024, p. 20) e che si intende con "direct applicability" «a method of incorporation of (secondary) [Union] Law into the municipal legal order» e, con "effetto diretto", «as to when a [Union] provision is susceptible of receiving judicial enforcement» (*ivi*, nota 62). V. *ivi* anche richiami a WINTER 1972.

80. V. QUINTAIS-APPELMAN-FATHAIGH 2023, p. 902; POLLICINO 2019, p. 12 ss.; POLLICINO 2018. Più in generale, sull'effetto orizzontale delle disposizioni costituzionali relative ai diritti inviolabili anche nei confronti delle piattaforme digitali private, v. NIRO 2021, p. 1383 ss., che segnala la preoccupazione derivante dall'attribuzione alle piattaforme online di poteri privati in competizione con gli attori pubblici, in quanto tale attribuzione potrebbe preludere ad una sostanziale "cessione" dello spazio della rete da parte delle autorità statali a favore delle piattaforme (p. 1391). Fa riferimento al "ruolo quasi pubblico" delle VLOP, anche CITINO 2022 (v. rinvio dell'Autore a vari Autori).

dell'Unione europea («Carta»), in particolare la libertà di espressione e di informazione, [...]».

Il considerando 40 chiarisce che «Al fine di conseguire gli obiettivi del presente regolamento, e in particolare per migliorare il funzionamento del mercato interno e garantire un ambiente online sicuro e trasparente, è necessario stabilire una serie chiara, efficace, prevedibile ed equilibrata di obblighi armonizzati in materia di dovere di diligenza per i prestatori di servizi intermediari. Tali obblighi dovrebbero in particolare mirare a conseguire diversi obiettivi di interesse pubblico quali [...] la tutela dei pertinenti diritti fondamentali sanciti dalla Carta, la significativa assunzione della responsabilità da parte di tali prestatori e il conferimento di maggiore potere ai destinatari e alle altre parti interessate, agevolando nel contempo la necessaria vigilanza da parte delle autorità competenti».

Il considerando 47 riconosce che «Nel progettare, applicare e far rispettare tali restrizioni, i prestatori di servizi intermediari dovrebbero agire in modo non arbitrario e non discriminatorio e tener conto dei diritti e degli interessi legittimi dei destinatari del servizio, compresi i diritti fondamentali sanciti dalla Carta. A titolo di esempio, i fornitori di piattaforme online di dimensioni molto grandi dovrebbero in particolare tenere debitamente conto della libertà di espressione e di informazione, compresi la libertà e il pluralismo dei media [...]».

L'art. 1, par. 1, prevede che «L'obiettivo del [...] regolamento è contribuire al corretto funzionamento del mercato interno dei servizi intermediari stabilendo norme armonizzate per un ambiente online sicuro, prevedibile e affidabile che faciliti l'innovazione e in cui i diritti fondamentali sanciti dalla Carta [...] siano tutelati in modo effettivo.».

L'art. 34, par. 1, secondo periodo, stabilisce che «La valutazione del rischio deve essere specifica per i loro servizi e proporzionata ai rischi sistemici, tenendo in considerazione la loro gravità e la loro

probabilità, e deve comprendere i seguenti rischi sistemici: [...] b) «Eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali, in particolare i diritti fondamentali alla [...] libertà di espressione e di informazione, inclusi la libertà e il pluralismo dei media, sanciti nell'articolo 11 della Carta [...] 28, 34 e 35 del DSA e all'art. 28 *ter* della Direttiva SMA».

L'art. 35, par. 3 dispone che «La Commissione, in cooperazione con i coordinatori dei servizi digitali, può emanare orientamenti sull'applicazione del paragrafo 1 in relazione a rischi concreti, con l'obiettivo specifico di presentare le migliori pratiche e raccomandare eventuali misure, tenendo debitamente conto delle possibili conseguenze di tali misure sui diritti fondamentali di tutte le parti interessate sanciti dalla Carta. Nell'elaborazione di tali orientamenti la Commissione organizza consultazioni pubbliche».

In questo contesto, risulta rilevante anche la giurisprudenza della Corte di Giustizia e della Corte EDU che estende la tutela della libertà di espressione persino «alle informazioni considerate false, nonché alle informazioni o idee che offendono, turbano o disturbano. Perciò, i contenuti generalmente considerati come disinformazione sono tutelati dalla libertà di espressione, con la conseguenza che un utente di servizi online ha, in linea di principio, il diritto di diffondere contenuti falsi senza interferenze da parte dei poteri pubblici»⁸¹.

Inoltre, l'articolo 52 della Carta prevede che: «[1.] Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. [2.] [...]»⁸².

81. PALUMBO-PIEMONTE 2024, p. 122 e la giurisprudenza citata alle note 28, 29, BASSINI-POLLICINO 2023, p. 435 ss.; CAGGIANO 2021, p. 11 ss.) Sulla disinformazione, v. POLLICINO-DUNN 2024; POLLICINO-DUNN 2024-A, p. 119 ss.; POLLICINO 2022, p. 89 ss. Sulle ragioni per cui i mezzi di informazione di massa forniscono informazioni sulle fake news, v. TSFATI-BOOMGAARDEN-STRÖMBÄCK et al. 2020.

82. Anche la CEDU (art. 10, co. 2) prevede delle condizioni all'esercizio della libertà di informazione purché queste siano stabilite dalla legge e costituiscano «misure necessarie, in una società democratica» ai sensi della stessa norma. BASSINI-POLLICINO 2023, p. 437 sottolineano che, anche se il *three step test* previsto dall'art. 10, co. 2

Secondo la Corte di Giustizia, in base a tale norma, l'atto che consente l'ingerenza in diritti e libertà fondamentali «deve definire, esso stesso, la portata della limitazione dell'esercizio del diritto considerato», cioè deve circoscrivere la portata della limitazione.⁸³

A riguardo, la formulazione degli obblighi del DSA a carico dei VLOPP (in specie quelli di cui all'art. 35) pone dubbi di conformità rispetto al principio di legalità di cui all'art. 52 della Carta per la sua vaghezza e la conseguente discrezionalità delle decisioni che tali soggetti possono assumere, sulla base delle loro condizioni generali, nei confronti dei contenuti diffusi attraverso le loro piattaforme⁸⁴.

Inoltre, la stessa attribuzione di potestà in qualche modo sanzionatorie ai VLOPP⁸⁵ nei confronti dei MSP solleva questioni di conformità al principio di legalità espresso dal suddetto art. 52.

Quanto al primo aspetto, la Corte di Giustizia ha precisato, da un lato, che il requisito della legalità «non esclude che la limitazione [...] sia formulata in termini sufficientemente ampi, in modo da potersi adattare a fattispecie diverse nonché ai cambiamenti di situazione, e, dall'altro, che la Corte può, se del caso, precisare, in via interpretativa, la portata concreta della limitazione in considerazione sia dei termini stessi della normativa dell'Unione di cui trattasi sia dell'impianto sistematico e agli obiettivi

deve essere interpretato restrittivamente, l'avvento di Internet ha comportato un aumento dei casi di restrizione della libertà di espressione, nonché un approccio da parte della Corte EDU teso a richiedere maggiori responsabilità agli organi di informazione considerati i rischi associati a internet per i diritti fondamentali. V. inoltre quanto ribadito dall'Assemblea parlamentare del Consiglio d'Europa, il 1° ottobre 2024 (*Report of the Committee on Culture, Science, Education and Media*, rapporteur: Mr Stefan Schennach), text adopted by the Assembly on 1st October 2024 (26th sitting): «Measures to fight against harmful propaganda must, however, respect the right to freedom of expression, including freedom of information [...]. As stated in the case law of the European Court of Human Rights, restrictions on this right must be provided by law, and be motivated by and proportionate to a legitimate aim.» (punto 3). Sentenza della Corte di Giustizia, cause riunite C-37/20 e C-601/20, 22 novembre 2022.

83. Sentenza della Corte di Giustizia, cause riunite C-37/20 e C-601/20, 22 novembre 2022.

84. V. *Report by the Special Rapporteur on the Promotion & Protection of the Right to Freedom of Op. & Expression*, U.N. Doc. A/HRC/38/35 (2018). Sulle critiche dello United Nations Special Rapporteur on freedom of expression v. QUINTAIS-APPELMAN-FATHAIGH 2023, «for their overly vague rules of operation, inconsistent enforcement, and overdependence on automation, which can lead to over-blocking and pre-publication censorship. This criticism is combined with, and amplified by, the notion that Big Tech exercises too much power over our online public sphere. Therefore, to better protect free expression online, the UN Special Rapporteur and civil society have argued platforms “should incorporate directly” principles of fundamental rights law into their terms and conditions (T&Cs)» (p. 882). Sul medesimo tema e sull'analogia con il GDPR, v. FOLKERT-KALÉDA-LOWENTHAL 2024, pp. 123-124. Sulla delega a un soggetto privato dell'interpretazione ed applicazione di tali principi e diritti, v. CERRINA FERONI 2024, «[...] non si può escludere che gli obblighi di valutazione e di attenuazione dei rischi sistemici previsti dagli artt. 34 e 35 del Regolamento possano avere un impatto non necessario e sproporzionato sulla libertà di espressione [...] il Regolamento conferisce a questi soggetti, di natura privatistica, il bilanciamento dei diritti e libertà fondamentali delle persone fisiche [...] senza circoscrivere in modo chiaro e specifico i margini di intervento per conformarsi agli obblighi imposti [...]». Pertanto l'effetto paradossale delle norme del Regolamento potrebbe essere quello di accrescere i margini di discrezionalità di tali soggetti privati, definiti non impropriamente “Stati dai confini immateriali” per la natura pubblicistica delle funzioni svolte». Su queste tematiche, v. anche PACULA 2024, pp. 259-274; FOLKERT-KALÉDA-LOWENTHAL 2024, p. 47; NIRO 2021, p. 1385 ss.; GRANDINETTI 2021; MARONI-BROGI 2021.

85. La disciplina settoriale dei media prevede la sospensione dell'attività trasmissiva, che rappresenta la sanzione più severa per i casi di “particolare gravità”. V. ad es. *Delibera AGCOM 152/20/CONS* che, per la parte relativa all'applicazione di tale sanzione, è stata annullata dal TAR Lazio in quanto carente di proporzionalità rispetto alla condotta contestata («consistente nella trasmissione del format televisivo ritenuto pregiudizievole per la salute, per due soli giorni di programmazione») (così TAR Lazio, 2 dicembre 2020, n. 12883/2020).

che essa persegue, come interpretati alla luce dei diritti fondamentali garantiti dalla Carta»⁸⁶.

In particolare, in una sentenza della Corte di Giustizia relativa agli obblighi delle piattaforme online di cui alla Direttiva DSM⁸⁷, e cioè relativa all'art. 17, è stato riconosciuto che «l'obbligo, per i fornitori di servizi di condivisione di contenuti online, di controllare i contenuti che gli utenti intendono caricare sulle loro piattaforme prima della loro diffusione al pubblico, derivante dal regime specifico di responsabilità introdotto dall'art. 17, c. 4, della direttiva 2019/790, e segnatamente dalle condizioni di esonero previste all'art. 17, c. 4, lett. b), e lettera c), è stato accompagnato dal legislatore dell'Unione da garanzie adeguate per assicurare, conformemente all'art. 52, paragrafo 1, della Carta, il rispetto del diritto alla libertà di espressione e d'informazione degli utenti di tali servizi, garantito all'art. 11 della Carta, nonché il corretto equilibrio tra tale diritto, da un lato, e il diritto di proprietà intellettuale, protetto all'art. 17, paragrafo 2, della Carta, dall'altro»⁸⁸.

Secondo la Corte di Giustizia, l'art. 17 della Direttiva DSM ed in specie i suoi parr. 7, 8, 9 e 10 forniscono, infatti, adeguate garanzie per la ricerca del giusto equilibrio⁸⁹.

In particolare, da tale norma si ricava che i contenuti che costituiscono esercizio di eccezioni o limitazioni ai diritti esclusivi (citazione, critica, rassegna, caricatura, parodia o pastiche) o comunque leciti (utilizzi riconosciuti come oggetto di un diritto soggettivo dell'utente ex art. 17, par. 7) non possono essere sistematicamente bloccati nel corso del loro caricamento in rete (né possono essere oggetto di sistematica rimozione permanente *ex post*).

A tal riguardo, la Corte richiama i paragrafi 164, 165 e da 191 a 193 delle Conclusioni dell'Avvocato Generale (che a loro volta sono preceduti da una serie di considerazioni) che afferma che occorre essere chiari in merito al fatto che la norma di cui all'art. 17, par. 7, della Direttiva DSM pone un obbligo di risultato e non di mezzi⁹⁰.

In tal senso, i prestatori di servizi di condivisione di contenuti online sono tenuti al risultato di non impedire la messa in rete sui loro servizi di contenuti che riproducono in maniera legittima opere o altri materiali protetti, anche qualora tali contenuti siano stati identificati dai titolari dei diritti. Le misure di blocco non devono dunque avere per oggetto o per effetto di impedire utilizzi legittimi.

Secondo la Corte di giustizia, le misure adottate a tal fine dal prestatore online devono essere «rigorosamente mirate» nel senso che devono riguardare i contenuti illeciti e non avere un effetto arbitrario o eccessivo sui contenuti leciti⁹¹.

Alla luce di quanto sopra, la fattispecie esaminata in tal caso dalla Corte di Giustizia appare diversa da quelle di cui agli artt. 28, 34 e 35 del DSA, dal momento che, come la Corte riconosce, nel primo caso non viene lasciata alla piattaforma online la determinazione dei rischi né tantomeno delle misure da adottare, anche se la stessa può scegliere la tecnologia o soluzione pratica più adatta per adempiere agli obblighi di contrasto alle utilizzazioni abusive in rete di contenuti protetti.

Infatti, le fattispecie sono descritte nell'art. 17 della Direttiva DSM e le misure sono quelle già determinate dalla stessa norma anche alla luce degli Orientamenti forniti dalla Commissione UE⁹².

Gli articoli del DSA lasciano invece alla determinazione dei VLOPP i rischi sistemici e le

86. Sentenza della Corte di Giustizia, 22 novembre 2022, cit.

87. Direttiva (UE) 2019/790 del 17 aprile 2019 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE ("Direttiva DSM").

88. Sentenza C-401/19, 26 aprile 2022, § 98 che richiama i §§ da 72 a 97.

89. § 80 ss. della sentenza.

90. § 85 della sentenza.

91. V. CILIBERTI 2022, p. 390.

92. Orientamenti sull'applicazione dell'art. 17 della direttiva (UE) 2019/790, Comunicazione della Commissione UE COM(2021) 288 final: «per determinare se un prestatore di servizi di condivisione di contenuti online si sia adoperato al meglio secondo elevati standard di diligenza professionale di settore, è particolarmente importante esaminare le pratiche di settore vigenti sul mercato in un dato momento. Ciò comprende l'uso della tecnologia o di soluzioni tecnologiche particolari. Come chiarito al considerando 66, "qualsiasi misura adottata dai prestatori di servizi dovrebbe essere efficace rispetto agli obiettivi perseguiti". I prestatori di servizi di condivisione di

conseguenti misure di mitigazione, senza una definizione *ex lege* di tali rischi e delle condizioni necessarie per l'adozione di tali misure, né tantomeno della portata di queste ultime⁹³. Inoltre, quanto alla moderazione dei contenuti, essa si basa sulle condizioni generali delle VLOP per le quali si pongono i problemi di vaghezza e discrezionalità sopra illustrati⁹⁴. La questione assume ancora più rilevanza considerando che gli obblighi a carico dei VLOPP di rispetto dei diritti fondamentali potrebbero essere intesi solo come di mezzi e non di risultato, con conseguente scusabilità di eventuali errori degli esiti derivanti dall'applicazione di tali mezzi⁹⁵.

In questa situazione, appare difficile per gli interessati prevedere se e quali restrizioni potrebbero essere imposte da un VLOPP ai contenuti di un MSP qualificato, e dunque alla sua libertà di espressione.

L'assenza di prevedibilità contrasta peraltro con gli obiettivi che lo stesso DSA si prefigge ai sensi dell'art. 1, par. 1⁹⁶.

Quanto al secondo aspetto, il riconoscimento di una "censura privata sostanziale" in cui il bilanciamento fra libertà di espressione e altri beni giuridici viene delegato dallo Stato alle piattaforme digitali può sollevare problematiche costituzionali dal momento che è necessario garantire la libertà dei media e il loro pluralismo anche sulle piattaforme online⁹⁷.

3. I servizi di media

Alla luce delle esposte considerazioni, si spiega la ragione per la quale l'Unione europea abbia ravvisato la necessità di inserire nell'EMFA alcune precisazioni riguardo alle attività dei VLOPP che potrebbero interferire con la diffusione dei contenuti online dei MSP⁹⁸.

contenuti online dovrebbero tuttavia rimanere liberi di scegliere la tecnologia o la soluzione più adatta per adempiere l'obbligo di diligenza nelle rispettive situazioni concrete» (§ 2).

93. V. PALUMBO-PIEMONTE 2024, «Partendo dalla sentenza della Corte sull'art. 17 della Direttiva DSM è anzi possibile argomentare che l'art. 35 non è pienamente conforme al principio di legalità, proprio in ragione della sua differente formulazione e differenti ricadute applicative rispetto all'art. 17 della Direttiva DSM» (p. 11) e che «la definizione dei rischi sistemici è un passaggio essenziale per determinare a quali condizioni l'art. 35 impone l'obbligo di adottare misure di mitigazione. Non solo non vi è una definizione legislativa di cosa si intenda per rischio sistemico, ma l'art. 34 è vago sulle modalità di individuazione di tali rischi» (p. 12).

94. V. anche *infra* paragrafo 5.

95. Secondo DEL MORAL SÁNCHEZ 2024, «This issue revolves around the question of whether the due diligence obligations addressed to users are obligations of means [...], or of result [...]. In other words, the debate is about whether the DSA establishes a series of procedural tools only, and thus platforms must comply with them but without an expectation of no-fault results. Individual mistakes could be regarded, for some obligations, as a possible margin of error in the mechanism provided for by the online service provider.» (p. 33). Inoltre, L'Autore sottolinea che, mentre gli obblighi di cui agli artt. 34 e 35 del DSA sono stabiliti "a favore" del regolatore e non degli utilizzatori di VLOP, quelli di cui all'art. 28 del DSA attribuiscono diritti direttamente in capo agli individui che sono beneficiari della sua previsione, ma «All in all, it could be argued that the manner the DSA is constructed, its objectives, and the rationale behind its rules, point to the direction that users are indeed entitled to expect, derived from the obligations of the DSA, not only the establishment of certain procedural mechanisms, but also the correct results in the application of those tools» (p. 35). In questo contesto, è importante un'interpretazione che assicuri agli utilizzatori di VLOP gli strumenti necessari alla tutela dei loro diritti (p. 36).

96. L'art. 1, par. 1 precisa che l'obiettivo del DSA è di stabilire «norme armonizzate per un ambiente online sicuro, prevedibile e affidabile» in cui i diritti fondamentali sanciti dalla Carta siano tutelati in modo effettivo.

97. Sul tema della delega di poteri ai VLOPP, v. anche GRANDINETTI 2022; MONTI 2019, p. 39 ss.; CERRINA FERONI 2024 che osserva che le piattaforme online sono definite «non impropriamente "Stati dai confini immateriali" per la natura pubblicistica delle funzioni svolte»; CONTI 2018, pp. 200-225.

98. Sul tentativo di inserire una "esenzione media" nel DSA, v. PAPAÉVANGELOU 2023, pp. 467 ss. L'emendamento proposto era il seguente: «Platforms shall not remove, disable access to, suspend or otherwise interfere with [content of press publications] or the related service or suspend or terminate the related account based on the alleged

L'obiettivo è, infatti, di rafforzare i diritti fondamentali dei MSP, poiché questi ultimi rappresentano operatori professionali specifici e ben individuabili nei singoli ordinamenti degli Stati membri⁹⁹.

In particolare, l'EMFA identifica i MSP sulla base di criteri che valgono a qualificarli ai fini dell'applicazione del *media privilege*.

Si tratta di una precisa scelta regolamentare dal momento che l'obiettivo è quello di «armonizzare alcuni aspetti delle norme nazionali relativi al pluralismo dei media e all'indipendenza editoriale»¹⁰⁰.

L'EMFA non si sofferma sull'oggetto del *media privilege*, limitandosi ad affermare che esso si applica ai servizi come «definiti dal TFUE e dovrebbe pertanto inglobare tutte le forme di attività economica. La definizione di servizi di media

dovrebbe comprendere in particolare le trasmissioni televisive o radiofoniche, i servizi di media audiovisivi a richiesta, i podcast audio o le pubblicazioni di carattere giornalistico. [...]. Inoltre, poiché l'attività dei fornitori di servizi di media nel mercato interno può assumere forme diverse, la definizione di fornitore di servizi di media dovrebbe coprire un'ampia gamma di operatori professionali dei media che rientrano nell'ambito della definizione di servizi di media, compresi i liberi professionisti.»¹⁰¹.

I contenuti di cui si occupa l'EMFA sono i prodotti informativi che rappresentano il risultato di «prestazioni di attività professionale svolte normalmente dietro compenso, finanziario o di altra

incompatibility of such content with [their] terms and conditions. (Art. 12b)». Tuttavia, «the final text, among others, adds media freedom and pluralism to the fundamental rights that digital platforms must respect, which was missing in the initial version proposed by the Commission» (*ivi*, p. 470); ASSOCIATION OF EUROPEAN RADIO 2022 (v. il link nell'articolo agli emendamenti che furono proposti dall'Associazione); BERTUZZI 2021; BUIJS 2021. Sulla necessità, con l'EMFA, di rimediare ad alcune carenze del DSA, v. EUROPEAN PUBLISHERS COUNCIL, *European Commission unveils bold and ambitious Media Freedom Act*, 16 September 2022. Per le critiche al *media privilege* poiché potrebbe rappresentare un ostacolo alla lotta alla disinformazione, v. EU DISINFOLAB 2023.

99. CESARINI-DE GREGORIO-POLICINO 2023. Inoltre, si noti che l'art. 18 dell'EMFA, ai sensi del suo par. 1, lett. d, si riferisce ai soli MSP comunque soggetti alla giurisdizione di uno Stato membro. La norma non appare estendersi ai MS «provenienti dall'esterno dell'Unione», che sono regolati all'art. 17. ERGA solleva dubbi sul perimetro della nozione di MS «provenienti dall'esterno dell'Unione» essendo cruciale che tale nozione si estenda «to unambiguously cover all types of media with links to foreign states» (v. ERGA recommendations for EMFA trilogues, cit., nel commento all'art. 16, lett. D). Sul tema delle emittenti televisive soggette al controllo di paesi terzi, v. anche SZÉP-WESSEL 2023, pp. 1384-1396; CILIBERTI 2022; LATTANZI 2022, p. 167 ss.; MAFFEO 2022, p. 195 ss.

100. Considerando 7 dell'EMFA.

101. V. Considerando 9 dell'EMFA che precisa quali siano i servizi esclusi, in particolare «i contenuti prodotti dagli utenti e caricati su una piattaforma online, a meno che tali contenuti non si configurino come prestazioni di attività professionale svolte normalmente dietro compenso, finanziario o di altra natura».

natura»¹⁰² e che sono riconducibili alla responsabilità di un editore¹⁰³.

L'EMFA non si occupa dunque dei contenuti informativi in sé, ma in quanto riconducibili ad un soggetto che ne assume la responsabilità editoriale¹⁰⁴.

L'EMFA stabilisce che il “servizio di media” è un «servizio quale definito agli articoli 56 e 57 TFUE, ove l'obiettivo principale del servizio stesso, o di una sua sezione distinguibile, sia la fornitura di programmi o di pubblicazioni di carattere

giornalistico, sotto la responsabilità editoriale di un fornitore di servizi di media, al grande pubblico, mediante qualsiasi mezzo, al fine di informare, intrattenere o istruire»¹⁰⁵.

In questa nozione ricadono i Servizi di Media Audiovisivi (“SMA”) come definiti all'articolo 1, paragrafo 1, lettera a), della direttiva 2010/13/UE¹⁰⁶; i servizi di media radiofonici¹⁰⁷ e le pubblicazioni di carattere giornalistico quali definite all'articolo 2, punto 4), della direttiva (UE) 2019/790¹⁰⁸.

102. V. artt. 1, par. 1 dell'EMFA e 4. L'EMFA garantisce l'autonomia delle entità che editano SMA, servizi radio o pubblicazioni giornalistiche e solo indirettamente dei singoli che forniscono informazioni di attualità. Per una critica a questo approccio v. CESARINI-DE GREGORIO-POLLICINO 2023, secondo i quali «the degree of protection offered to media actors should be designed in such a way as to reflect their “public watchdog” role, which should not be restricted to traditional media but extended without discriminations to all actors that deploy a comparable role in the wider, and increasingly digital, information space» (par. 3.1); «prerogatives pertaining to freedom of expression apply not only to media organisations “but also to every person engaged in journalism”, and that journalistic activities include all types of communication whose purpose “is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them”» (*ibidem*). A riguardo, è stato anche osservato che la mancanza della definizione di “giornalista” all'interno dell'EMFA potrebbe generare dubbi sull'inclusione dei freelancer nel suo campo di applicazione (v. *Proposal of the Commission for a European Media Freedom Act (EMFA)*, *ERGA position*, cit., nel commento all'art. 4 della Proposta di DSA, lett. G.)). Tuttavia, per i contributi giornalistici di tali soggetti che facciano parte di un MS, si potrebbe configurare una copertura da parte dell'art. 18 dell'EMFA. V. anche la giurisprudenza della Corte EDU che estende ai giornalisti non di professione l'obbligo di agire in buona fede quando intervengono nel dibattito pubblico (*Braun v Poland*, 4 Febbraio 2015, § 40), nonché la Corte di Giustizia che ha riconosciuto che la ripresa, registrazione e la pubblicazione di un video da loro realizzate possono avere una finalità giornalistica (così sentenza C-345/17, 14 febbraio 2019). Sulla nozione piuttosto ampia di “pubblicazione di carattere giornalistico”, v. art. 2, punto 4, della direttiva (UE) 2019/790 cui rinvia l'art. 2, par. 1, punto 5 dell'EMFA. V. su tali temi, anche CUNIBERTI 2022, p. 265 ss.; PAPA-EVANGELOU 2023, pp. 473-476; TAMBINI 2021, pp. 523-539. Per completezza, si osserva che l'EMFA utilizza espressioni che denotano l'ampiezza dei soggetti coinvolti nella produzione di contenuti informativi, v. considerando 20-24 art. 4, parr. 3 e 8.

103. In Europa, la libertà dei media assume particolare rilevanza anche rispetto alla libertà di parola, in considerazione del ruolo di amplificazione che i media rivestono nella democrazia (così MUTO 2022, p. 222).

104. L'EMFA ha infatti introdotto un “safe harbour for editorial contents” (così CESARINI-DE GREGORIO-POLLICINO 2023, par. 2. *The Structure and Rationale*).

105. Art. 2, par. 1, punto 1. V. anche *supra* nota 104.

106. Ovvero «i) un servizio quale definito agli articoli 56 e 57 del trattato sul funzionamento dell'Unione europea, ove l'obiettivo principale del servizio stesso o di una sua sezione distinguibile sia la fornitura di programmi al grande pubblico, sotto la responsabilità editoriale di un fornitore di servizi di media, al fine di informare, intrattenere o istruire, attraverso reti di comunicazioni elettroniche ai sensi dell'articolo 2, lettera a), della direttiva 2002/21/CE; per siffatto servizio di media audiovisivo si intende o una trasmissione televisiva come definita alla lettera e) del presente paragrafo o un servizio di media audiovisivo a richiesta come definito alla lettera g) del presente paragrafo; ii) una comunicazione commerciale audiovisiva».

107. Che non sono espressamente coperti dalla Direttiva SMA. V. *supra* nota 10 e *infra* nota 113.

108. Ovvero «un insieme composto principalmente da opere letterarie di carattere giornalistico ma che può includere anche altre opere o altri materiali, e che: a) costituisce un singolo elemento all'interno di una pubblicazione

Il Regolamento EMFA fornisce anche la definizione di “decisione editoriale”. È tale «una decisione presa periodicamente al fine di esercitare la responsabilità editoriale e collegata alle attività quotidiane del fornitore di servizi di media»¹⁰⁹.

Qualifica, inoltre, la “responsabilità editoriale” come «l'esercizio di un controllo effettivo sia sulla selezione dei programmi o delle pubblicazioni di carattere giornalistico sia sulla loro organizzazione, ai fini della fornitura di un servizio di media, a prescindere dall'esistenza di una responsabilità ai sensi del diritto nazionale per il servizio fornito»¹¹⁰.

Il controllo deve essere effettivo da parte del soggetto che si dichiara editore del servizio e deve esserlo per entrambi gli aspetti: selezione dei contenuti e loro organizzazione. La riconducibilità di tali prerogative in capo a un soggetto diverso da quello che si dichiara editore del servizio o l'assenza di una di queste caratteristiche richiede un'attenta valutazione per individuare, nel primo caso, l'effettivo editore del servizio e, nel secondo, per comprendere se si sia effettivamente in presenza di un servizio di media¹¹¹.

Le elencate definizioni derivano dalla Direttiva SMA e vengono estese al settore della stampa, che però si presenta più articolato di quello dei SMA¹¹².

In particolare, un fornitore di SMA riconoscerà nella nozione di “responsabilità editoriale”, come sopra declinata, una delle caratteristiche essenziali della propria attività¹¹³. Infatti, la nozione di responsabilità editoriale è stata oggetto di ampie riflessioni in ambito europeo con riferimento ai fornitori di SMA e rappresenta un concetto consolidato.

A questo riguardo, in uno studio piuttosto risa-lente, ma tutt'ora di interesse, si afferma che «It is almost impossible to conceive of editorial services that manage without a controlling body, which would have to be defined as a service provider»¹¹⁴.

Un Servizio di Media Audiovisivo è, quindi, tale in quanto sia identificabile un soggetto al quale ricondurre la selezione dei contenuti e la loro organizzazione in un palinsesto o in un catalogo. Tale soggetto è il Fornitore di SMA (FSMA).

Per i contenuti giornalistici, siano essi forniti attraverso uno SMA o indipendentemente da questo, invece la nozione di “responsabilità editoriale” è più articolata perché, da un lato, vi sono i giornalisti e la relativa testata, e, dall'altro lato, l'editore che, nel primo caso (e cioè se il prodotto giornalistico sia incluso nella programmazione di uno SMA), sarà il FSMA.

periodica o regolarmente aggiornata recante un unico titolo, quale un quotidiano o una rivista di interesse generale o specifico; b) ha lo scopo di fornire al pubblico informazioni su notizie o altri argomenti; e c) è pubblicata su qualsiasi mezzo di comunicazione ad iniziativa e sotto la responsabilità editoriale e il controllo di un prestatore di servizi. Le pubblicazioni periodiche a fini scientifici o accademici, quali le riviste scientifiche, non sono pubblicazioni di carattere giornalistico ai sensi della presente direttiva».

109. La Direttiva SMA definisce la “decisione editoriale” sostanzialmente allo stesso modo.

110. La Direttiva SMA definisce la “responsabilità editoriale” sostanzialmente allo stesso modo.

111. Infatti, nel secondo caso potremmo essere in presenza di una PCV (Piattaforma di Condivisione di Video), poiché per quest'ultima si richiede solo l'organizzazione dei contenuti e non la loro selezione. V. a riguardo, CILIBERTI 2024; NIKOLTCHEV 2008, p. 26.

112. Sulle diversità esistenti tra le regolamentazioni nazionali, v. CANTERO GAMITO 2022, p. 3 ss. Con particolare riferimento ai prodotti giornalistici, l'Autrice osserva che «self-regulation by journalists and other media professionals has been a significant tool in the media sector to limit state interference. Due to the potential of self-regulatory professional and ethical standards for governing the industry and preserving its autonomy, the legislator has recognised and even mandated self-regulation in the sector» (p. 8). Sempre sulle diversità esistenti tra le regolamentazioni nazionali, v. Raccomandazione (UE) 2022/1634, cit., e in particolare i considerando 12-19 e artt. 4-14; MUTO 2022, che sottolinea che «tali differenze producono effetti negativi con riferimento alla tutela delle fonti, all'incertezza del diritto connessa alla loro responsabilità legale ed amministrativa» (p. 229).

113. Lo stesso vale per il fornitore di servizi radiofonici per il quale non viene fornita una specifica definizione nell'EMFA. Si ricorda che tale attività non è oggetto di armonizzazione nella Direttiva SMA, mentre il TUSMA include più riferimenti alla nozione di servizio radiofonico.

114. NIKOLTCHEV 2008, p. 4.

In base all'ordinamento giuridico italiano, la testata giornalistica, sia essa all'interno di uno SMA oppure al di fuori di questo, gode di indipendenza e autonomia nei rapporti con il proprio editore così che il giornalista non dovrebbe ricevere dirette indicazioni sullo svolgimento della propria attività professionale dall'editore, bensì solo dai superiori gerarchici inquadrati nella sua redazione¹¹⁵.

A questo riguardo, in Italia, il Testo Unico dei doveri del giornalista riconosce che «il giornalista [...] accetta indicazioni e direttive soltanto dalle gerarchie redazionali, purché le disposizioni non siano contrarie alla legge professionale, al contratto nazionale di lavoro e alla deontologia professionale».

I rapporti tra l'editore, la testata e i suoi componenti sono fondati su due rapporti fiduciari: da un lato, tra l'editore e il direttore e, dall'altro lato, tra la redazione, rappresentata a tal fine dal comitato di redazione, e il direttore.

Più in particolare, è il direttore della testata che stipula con l'editore un accordo che definisce la linea politica, l'organizzazione e lo sviluppo della

testata ed è il direttore della testata a dare comunicazione di tali direttive alla redazione, attraverso i comitati o fiduciari di redazione¹¹⁶.

In ciascuno Stato membro tale relazione potrebbe avere proprie specificità, come riconosciuto negli stessi considerando dell'EMFA¹¹⁷, ma quelli sopra descritti dovrebbero essere tratti comuni¹¹⁸.

Ne consegue che la nozione di "responsabilità editoriale", con riguardo al settore della stampa, deve essere necessariamente adattata alle norme dei singoli ordinamenti disciplinanti l'attività giornalistica (come modificate a seguito dell'entrata in vigore dell'EMFA) sia che il risultato di tali attività (le "pubblicazioni giornalistiche") sia parte di un Servizio di Media Audiovisivo (tipicamente, attraverso notiziari) o che consista in un prodotto a sé stante comunque riconducibile ad un editore.

Ai fini dell'EMFA, potrebbero essere di aiuto ad individuare i prodotti informativi riconducibili a un MSP le informazioni aggiornate sul «loro nome legale o i loro nomi legali e i loro dati di contatto» che l'editore è tenuto a rendere facilmente e direttamente accessibili ai destinatari dei loro servizi¹¹⁹. In

115. FLORE 2023, p. 251 ss.; CUNIBERTI 2022, p. 280 ss.

116. Per indicazioni più puntuali sui rapporti tra editore, direttore, comitato di redazione e intero corpo redazionale, v. il CCNLG-Contratto Collettivo Nazionale di Lavoro Giornalistico. In generale, la figura del direttore è il vero *trait d'union* tra impresa e giornalisti, mentre il comitato di redazione svolge un importante ruolo di garanzia a favore di questi ultimi.

117. Considerando 5, 18 e, sulla necessità comunque di adottare misure per preservare il rispetto degli standard di indipendenza durante l'intero processo editoriale all'interno dei media anche al fine di salvaguardare l'integrità dei contenuti giornalistici, considerando 34 e 35.

118. Sono utili alla conoscenza dei singoli ordinamenti, gli standard della *Journalism Trust Initiative* o gli standard delle organizzazioni della società civile, delle organizzazioni di fact-checking e altre organizzazioni professionali *pertinenti* (considerando 53 dell'EMFA). V. anche *International Federation of Journalists Code*, nonché la Raccomandazione (UE) 2022/1634, cit. della Commissione del 16 settembre 2022 sulle garanzie interne di indipendenza editoriale e la trasparenza della proprietà nel settore dei media, cit., nonché considerando 34 dell'EMFA. Con riguardo ai diversi regimi nazionali, v. BROUGHTON MICOVA-SCHNURR-CALEF-ENSTONE 2024, che segnalano che: «content from sources that fall under regulatory or self-regulatory regimes is not necessarily free from risk. There are self-regulatory systems across Europe that struggle to enforce ethical standards and member states whose regulatory authorities' independence is challenged» (p. 32). Per questa ragione, ai fini del beneficio del *media privilege*, i MSP devono anche possedere il requisito dell'indipendenza. In particolare, se forniscono notizie e contenuti di attualità, devono dichiarare di aver adottato «le misure che ritengono appropriate al fine di garantire l'indipendenza delle decisioni editoriali. In particolare, tali misure mirano a garantire che: a) le decisioni editoriali possano essere adottate liberamente nell'ambito della linea editoriale stabilita del fornitore di servizi di media interessato; e b) qualsiasi conflitto di interessi, effettivo o potenziale, che possa influenzare la fornitura di notizie e contenuti di attualità sia comunicato» (art. 18, co. 1 dell'EMFA). V. *supra* nota 15 per gli altri requisiti richiesti ai MS.

119. Art. 6 dell'EMFA.

questo modo, in presenza anche solo di un singolo contenuto informativo, sarebbe possibile comprendere se lo stesso sia riconducibile ad un MSP.

Inoltre, per le ragioni che saranno meglio descritte di seguito, sarebbe anche utile che il contenuto online includesse una dicitura per identificare il nome dello SMA (palinsesto o catalogo)¹²⁰ o della pubblicazione periodica o regolarmente aggiornata, quale un quotidiano o una rivista di interesse generale o specifico¹²¹, da cui il singolo contenuto sia stato tratto e diffuso su una VLOP.

Infatti, l'art. 18, par. 1, lett. d) dell'EMFA richiede che il MSP, per qualificarsi ai fini del *media privilege*, debba essere soggetto a regolamentazione, autoregolamentazione o coregolamentazione «ampiamente riconosciuta[o] e accettata[o] nel pertinente settore dei media» e alla supervisione di un'Autorità o di un organismo competente di regolamentazione, coregolamentazione o autoregolamentazione.

Ora, il contenuto di un MS pubblicato su una VLOP potrebbe sfuggire alla regolamentazione di settore, pur essendo il relativo MSP qualificato ai sensi dell'art. 18, par. 1 dell'EMFA.

Ad esempio, non tutti i contenuti di FSMA sono soggetti ad autorizzazione da parte dell'Autorità di regolamentazione e, in tal caso, non dovrebbe essere applicabile la disciplina settoriale, ferma restando la normativa generale valida per qualsiasi contenuto diffuso al pubblico¹²².

Così i canali televisivi, soggetti alla giurisdizione italiana, diffusi su "altri mezzi diffusione" (e cioè su mezzi diversi da satellite e da terrestre) non sono soggetti ad autorizzazione se di durata inferiore a 24 ore settimanali, se non includono almeno due notiziari o se non abbiano un numero minimo di due addetti¹²³.

In tali casi, il servizio di media audiovisivo, anche se ricadente nella nozione di SMA, non è soggetto ad autorizzazione e dunque, a stretto rigore, non dovrebbe essere soggetto ad obblighi regolamentari.

I contenuti che fossero diffusi su tali canali, e che non fossero diffusi su altri canali dello stesso editore soggetti a regime amministrativo, potrebbero non ricadere nel *media privilege* anche laddove il fornitore di tale servizio renda accessibile la propria denominazione e i dati di contatto o, comunque, potrebbero essere soggetti ad una gestione più attenta da parte dei VLOPP, ferma la tutela dei diritti fondamentali dei SMA.

Inoltre, vi sono servizi audiovisivi che, pur non essendo soggetti ad autorizzazione, sono destinatari di regolamentazione. Così, ad esempio, accade in Italia per i servizi on line degli *influencer*. Infatti, se da un lato i servizi online degli *influencer* che soddisfano tutti i requisiti per essere qualificati come FSMA (in particolare come FSMA "a richiesta") sono soggetti al regime autorizzativo stabilito dalla Delibera 295/23/CONS e a tutte le norme

120. Nella Direttiva SMA non è presente una nozione di "palinsesto" (viene fornita la nozione di «radiodiffusione televisiva» o «trasmissione televisiva») né di "catalogo" (viene fornita la nozione di «servizio di media audiovisivo a richiesta»). V. rispettivamente, art. 1, par. 1, lett. e) e g) della Direttiva SMA.

121. Il riferimento alla «pubblicazione periodica o regolarmente aggiornata recante un unico titolo, quale un quotidiano o una rivista di interesse generale o specifico» è tratto dalla definizione di «pubblicazioni di carattere giornalistico» di cui all'art. 2, punto 4), della Direttiva DSM.

122. In Italia non tutti i contenuti riconducibili a un fornitore di SMA sono soggetti alla regolamentazione di settore. Infatti, potrebbero esserci palinsesti inferiori alle 24 ore settimanali che sfuggono ai regimi autorizzativi, così come contenuti realizzati dall'editore e che vengono diffusi online, ma che non sono anche inclusi in un palinsesto televisivo o in un catalogo a richiesta. In tali casi, i contenuti del FSMA, pur riconducibili ad un soggetto che può astrattamente fornire la dichiarazione ai sensi dell'art. 18, par. 1, lett. a), b), c), e), f) e g) dell'EMFA, potrebbero non essere soggetti alle prescrizioni normative di cui alla lett. d) di tale articolo. Si v. meglio *infra* al paragrafo 3. In merito alla disciplina dei SMA, v. CILIBERTI 2024. Con riguardo ai prodotti giornalistici riconducibili a un editore soggetto alla giurisdizione nazionale, la questione potrebbe avere minor rilievo dal momento che tali prodotti ricadono nella disciplina indicata *supra* alla nota 13 e semmai il tema potrebbe essere la loro riconducibilità a un soggetto che se ne assuma la responsabilità come editore.

123. Art. 4, allegato A alla [Delibera AGCOM 295/23/CONS](#) di approvazione del Regolamento concernente la disciplina relativa al rilascio dei titoli autorizzatori alla fornitura di servizi di media audiovisivi e radiofonici via satellite, su altri mezzi di comunicazione elettronica e a richiesta.

del TUSMA applicabili ai SMA a richiesta, dall'altro lato quelli che non soddisfano tutti i requisiti previsti per essere qualificati come SMA sono comunque destinatari di Linee Guida dell'Autorità per le Garanzie nelle Comunicazioni¹²⁴ se svolgono un'attività analoga o assimilabile a quella dei FSMA e nella misura in cui soddisfino cumulativamente una serie di requisiti individuati dalla stessa AGCOM (cd. *influencer* professionali)¹²⁵. La qualificazione di un servizio online di un *influencer* come SMA o come servizio assimilabile ad uno SMA assume, pertanto, rilevanza ai fini dell'applicazione del *media privilege*, indipendentemente dal fatto che tale servizio sia soggetto o meno a regime autorizzativo¹²⁶.

Analoghe considerazioni potrebbero porsi per i contenuti informativi, pubblicati online con l'indicazione del relativo editore qualificato ai sensi dell'art. 18, par. 1 dell'EMFA, ma non riconducibili a una sua pubblicazione periodica o regolarmente aggiornata¹²⁷.

In conclusione, alla luce del combinato disposto delle norme esaminate, si ritiene ragionevole sostenere che l'inapplicabilità del *media privilege* ai sensi dell'articolo 18, paragrafo 4, ult. co., possa riguardare esclusivamente i contenuti che, pur essendo attribuibili a MSP qualificati, non siano soggetti alle prescrizioni normative o regolamentari del pertinente Stato membro (in particolare per quanto riguarda i SMA), o che non siano tratte

da, o comunque non siano collegate a, "pubblicazioni di carattere giornalistico" degli stessi MSP.

4. Le piattaforme online e le piattaforme televisive

Le piattaforme online hanno assunto un ruolo importante nella circolazione di informazioni in quanto hanno consentito la disintermediazione dei rapporti tra l'editore e l'utente finale.

Attraverso le reti online, possono transitare contenuti di ogni genere, quali l'audiovisivo, il solo audio o testi, accompagnati o meno da immagini. Il finanziamento di tali contenuti può avvenire attraverso rapporti diretti con gli utenti, con gli inserzionisti o con le piattaforme online¹²⁸.

L'EMFA definisce la piattaforma online mediante un rinvio al DSA. Infatti, è tale quella «definita all'articolo 3, lettera i), del regolamento (UE) 2022/2065»¹²⁹, e cioè «un servizio di memorizzazione di informazioni che, su richiesta di un destinatario del servizio, memorizza e diffonde informazioni al pubblico, tranne qualora tale attività sia una funzione minore e puramente accessoria di un altro servizio o funzionalità minore del servizio principale e, per ragioni oggettive e tecniche, non possa essere utilizzata senza tale altro servizio e a condizione che l'integrazione di tale funzione o funzionalità nell'altro servizio non sia un mezzo per eludere l'applicabilità del presente regolamento».

124. Linee-guida volte a garantire il rispetto delle disposizioni del Testo unico da parte degli *influencer* e istituzione di un apposito Tavolo tecnico, approvate con [Delibera AGCOM 7/24/CONS](#).

125. Gli *influencer* amatoriali sono, invece, indirettamente soggetti alle norme del TUSMA, in particolare a quelle di cui agli artt. 41 e 42 TUSMA applicabili direttamente alle Piattaforme di Condivisione Video.

126. Infatti, come visto, in Italia un servizio online di un *influencer* assimilabile a uno SMA non è soggetto ad autorizzazione e, tuttavia, è destinatario di una disciplina simile a quella di uno SMA, pur con alcune differenze dovute alla particolarità del settore.

127. V. *supra* nota 108 che riporta la definizione di "pubblicazioni di carattere giornalistico".

128. Sui diversi modelli di business, v. BROUGHTON MICOVA-SCHNURR-CALEF-ENSTONE 2024, pp. 18-19.

129. Art. 2, par. 1, p. 9 che definisce così la piattaforma online: «piattaforma online quale definita all'articolo 3, lettera i)» del DSA. Quest'ultimo articolo la definisce nel seguente modo: «un servizio di memorizzazione di informazioni che, su richiesta di un destinatario del servizio, memorizza e diffonde informazioni al pubblico, tranne qualora tale attività sia una funzione minore e puramente accessoria di un altro servizio o funzionalità minore del servizio principale e, per ragioni oggettive e tecniche, non possa essere utilizzata senza tale altro servizio e a condizione che l'integrazione di tale funzione o funzionalità nell'altro servizio non sia un mezzo per eludere l'applicabilità del presente regolamento».

Si tratta di una nozione ampia, che include quella di Piattaforma di Condivisione di Video di cui alla Direttiva SMA¹³⁰ e quella di Prestatore di servizi di condivisione di contenuti online di cui alla Direttiva DSM¹³¹, e che nulla ha a che vedere con quella di MS, essendo quest'ultima tutta incentrata sulla responsabilità editoriale¹³².

Infatti, la piattaforma online, come definita ai sensi del DSA, svolge principalmente un'attività di memorizzazione e diffusione, su richiesta del destinatario del servizio, di informazioni al pubblico¹³³, con esclusione dei casi in cui tale attività «sia una funzione minore e puramente accessoria

di un altro servizio o funzionalità minore del servizio principale e, per ragioni oggettive e tecniche, non possa essere utilizzata senza tale altro servizio e a condizione che l'integrazione di tale funzione o funzionalità nell'altro servizio non sia un mezzo per eludere l'applicabilità» del DSA¹³⁴.

Prima delle piattaforme online, nel settore dei media esistono già delle «piattaforme», e cioè quelle che operano in particolare nel settore televisivo. L'esperienza regolamentare maturata nei loro confronti può essere utile ad affrontare i temi di questo contributo¹³⁵.

130. Con «servizio di piattaforma per la condivisione di video» si intende «un servizio quale definito agli articoli 56 e 57 del trattato sul funzionamento dell'Unione europea, ove l'obiettivo principale del servizio stesso, di una sua sezione distinguibile o di una sua funzionalità essenziale sia la fornitura di programmi, video generati dagli utenti o entrambi per il grande pubblico, per i quali il fornitore della piattaforma per la condivisione di video non ha responsabilità editoriale, al fine di informare, intrattenere o istruire attraverso reti di comunicazioni elettroniche ai sensi dell'articolo 2, lettera a), della direttiva 2002/21/CE e la cui organizzazione è determinata dal fornitore della piattaforma per la condivisione di video, anche con mezzi automatici o algoritmi, in particolare mediante visualizzazione, attribuzione di tag e sequenziamento». La Commissione europea ha fornito Orientamenti per l'applicazione pratica del criterio di «funzionalità essenziale» (2020/C 223/02).

131. Con tale nozione si intende «un prestatore di servizi della società dell'informazione il cui scopo principale o uno dei principali scopi è quello di memorizzare e dare accesso al pubblico a grandi quantità di opere protette dal diritto d'autore o altri materiali protetti caricati dai suoi utenti, che il servizio organizza e promuove a scopo di lucro» (art. 2, par. 1, n. 6 della Direttiva DSM).

132. V. *supra* note 13 e 110 e *infra* nota 137. Inoltre, si consideri che «in un ambiente mediatico sempre più convergente, alcuni fornitori di piattaforme per la condivisione di video o i fornitori di piattaforme online di dimensioni molto grandi hanno cominciato a esercitare un controllo editoriale su una o più sezioni dei loro servizi. Quando esercitano il controllo editoriale su una o più sezioni dei loro servizi, tali fornitori potrebbero quindi essere definiti sia come fornitori di piattaforme per la condivisione di video o come fornitori di piattaforme online di dimensioni molto grandi sia come fornitori di servizi di media.» (considerando 11 dell'EMFA).

133. Il DSA riconosce che le piattaforme online, quali i social network o i mercati online, devono essere definite come prestatori di servizi di hosting che non solo memorizzano informazioni fornite dai destinatari del servizio su richiesta di questi ultimi, ma diffondono anche tali informazioni al pubblico, sempre su richiesta di tali destinatari. In base al DSA «Il concetto di «diffusione al pubblico» [...] dovrebbe implicare la messa a disposizione di informazioni a un numero potenzialmente illimitato di persone [...]» (considerando 14). V. artt. 19-28 per le norme aggiuntive applicabili alle piattaforme online in ragione delle loro peculiarità.

134. V. art. 3, par. 1, lett. i del DSA.

135. «A queste osservazioni non varrebbe obiettare che le sfide poste dalle piattaforme sono senza precedenti nella storia dell'informazione e che non va compiuto l'errore di guardare ad esse utilizzando vecchi schemi [...] ed ancora che oggi non sono più i media ad essere gli intermediari, vendendo invece essi intermediati dalle piattaforme. Infatti, qui non si vuole affatto proporre di applicare acriticamente le stesse regole ai nuovi intermediari, quanto piuttosto di prendere atto che, ferma restando la necessità di applicare strumenti di tutela adatti ai nuovi attori, alcuni problemi di fondo sollevati dalle piattaforme possono trovare un buon punto di partenza nella pluriennale elaborazione sui media, tanto più che l'inapplicabilità ad esse dell'art. 21 Cost. consente un più ampio intervento sulle piattaforme.» (così GRANDINETTI 2022-A).

Non esiste una definizione codificata di piattaforma televisiva a livello nazionale o europeo¹³⁶.

Tale nozione può ricavarsi, anche solo indirettamente, da alcuni atti normativi, quali la Direttiva SMA¹³⁷, il Codice europeo sulle comunicazioni elettroniche¹³⁸ e la direttiva sulla fornitura di contenuto digitale e di servizi digitali¹³⁹.

La piattaforma televisiva svolge essenzialmente un'attività economica consistente nell'offerta di bouquet (e cioè pacchetti) composti da SMA riconducibili alla responsabilità editoriale della piattaforma televisiva stessa (che, per questo aspetto, assume anche la distinta qualità di editore)¹⁴⁰ e/o alla responsabilità di terzi editori, autonomi

136. Se si guarda ad alcuni precedenti in ambito antitrust è possibile desumere che la terzietà dei servizi di media audiovisivi offerti attraverso una piattaforma televisiva viene implicitamente assunta. Ad esempio, in passato la Commissione europea aveva ritenuto che l'accesso alla piattaforma costituisse «un elemento essenziale per facilitare i nuovi ingressi sul mercato della pay-TV e per consentire la trasmissione DTH dei canali a pagamento e in chiaro.» (punto 137 della Decisione della Commissione del 2 aprile 2003, caso [COMP/M.2876](#) – NewsCorp/Telepiù). La Commissione europea incentrava le sue preoccupazioni concorrenziali sui possibili ostacoli all'accesso alla piattaforma televisiva per un servizio di media audiovisivo terzo. V. anche altre decisioni della Commissione europea: NewsCorp/Premiere, del 25 giugno 2008 (caso [COMP/M.5121](#)); British Interactive Broadcasting/Open, del 15 settembre 1999 (caso [IV/36.359](#)); Bertelsmann/Kirch/Premiere, del 27 maggio 1998 (caso [IV/M.993](#)); MSG Media Service, del 9 novembre 1994 (caso [IV/M.469](#)). Su questi temi, v. GRANDINETTI 2012, p. 735 ss. Sulla distinzione dei ruoli, v. art. 5, co. 4 e 7, co. 2 del Regolamento in materia di obblighi di programmazione ed investimento a favore di opere europee e di opere di produttori indipendenti (Allegato A alla [Delibera AGCOM 424/22/CONS](#)).

137. In base alla Direttiva SMA, l'elemento caratterizzante un fornitore di SMA è la responsabilità editoriale con riguardo alla scelta dei singoli contenuti e alla loro organizzazione in un palinsesto o in un catalogo a richiesta. La piattaforma televisiva non seleziona invece i contenuti di un canale televisivo o di un servizio a richiesta né li organizza all'interno dei relativi palinsesti o cataloghi. Infatti, la piattaforma televisiva individua sul mercato i SMA che potrebbero comporre la sua offerta, ad esempio, secondo i target di utenti che intende raggiungere. Individua così i generi e la tematicità dei SMA di proprio interesse e negozia accordi di licenza con i relativi editori. Ogni responsabilità sulla natura ed i contenuti dei programmi diffusi mediante i SMA rimane in capo ai relativi editori, come emerge anche dalle autorizzazioni rilasciate da AGCOM per la loro diffusione. Infatti, tali autorizzazioni sono rilasciate agli editori dei canali o, a seconda dei casi, dei servizi a richiesta (v. [elenco autorizzazioni](#) presente sul sito AGCOM). È su questi ultimi soggetti che grava il rispetto degli obblighi stabiliti dalla normativa di settore, come risulta anche dal Regolamento AGCOM concernente la disciplina relativa al rilascio dei titoli autorizzatori alla fornitura di servizi di media audiovisivi cit. *supra* note 122-123. A quest'ultimo riguardo, v. anche *supra* nota 136 in merito al Regolamento in materia di obblighi di programmazione e investimento in opere europee.

138. V. Direttiva (UE) 2018/1972 dell'11 dicembre 2018 che istituisce il Codice europeo delle comunicazioni elettroniche. A tale riguardo, il Consiglio di Stato in una sentenza riconosce che: «la direttiva aveva ritenuto necessario “separare la disciplina dei mezzi di trasmissione dalla disciplina dei contenuti”, con la conseguenza che quel quadro normativo non trovava applicazione “ai contenuti dei servizi forniti mediante reti di comunicazione elettronica che utilizzano servizi di comunicazione elettronica, come i contenuti delle emissioni radiotelevisive, i servizi finanziari e taluni servizi della società dell'informazione e lascia quindi impregiudicate le misure adottate a livello comunitario o nazionale riguardo a tali servizi in ottemperanza alla normativa comunitaria, per promuovere la diversità culturale e linguistica e per assicurare la difesa del pluralismo dei mezzi di informazione” [considerandum n. 5; v., ora, il considerandum n. 7 della Direttiva 2018/1972 [...]]» (così sentenza Consiglio di Stato n. 04403/2024, del 17 maggio 2024).

139. Direttiva (UE) 2019/770 del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, che, con riguardo a tali contratti, individua la figura dello “operatore economico” (art. 2, par. 1, punto 5).

140. V. a riguardo, CILIBERTI 2023, p. 108 ss.

editorialmente dalla piattaforma. Vi potrebbero anche essere MS sulle Electronic Program Guide¹⁴¹ di una piattaforma televisiva che non sono parti del bouquet commerciale della stessa piattaforma¹⁴².

Con riguardo alla natura giuridica della piattaforma televisiva, il giudice nazionale ha recentemente riconosciuto che il servizio di una piattaforma televisiva «resta, giuridicamente, altro dalla definizione di servizi elettronici contenuta nella legge»¹⁴³.

Né, d'altro canto, la piattaforma televisiva è suscumbibile nella qualificazione di SMA dal momento che non sussiste, quantomeno ai sensi della disciplina di settore nazionale, un dovere o potere di controllo delle piattaforme televisive che gestiscono i bouquet sui contenuti (canali televisivi o cataloghi) riconducibili a editori terzi. Infatti, come esposto, dal punto di vista regolamentare, sono solo i FSMA ad essere responsabili del rispetto degli obblighi previsti dal TUSMA.

Per completezza, si osserva che, con riferimento a specifiche attività, quali quelle relative al fornitore di «servizi interattivi associati o di servizi di accesso condizionato o all'operatore di rete o di servizi sulla cui piattaforma o infrastruttura sono veicolati programmi»¹⁴⁴ – che non sono attività

necessariamente svolte da una piattaforma televisiva¹⁴⁵ – AGCOM può «disporre la sospensione della ricezione o ritrasmissione dei servizi sottoposti alla giurisdizione italiana [...] o non soggetti alla giurisdizione di alcuno Stato membro dell'Unione europea, i cui contenuti o cataloghi sono ricevuti direttamente o indirettamente dal pubblico italiano», dopo il formale richiamo ad adottare tutte le misure necessarie per impedire la diffusione di tali programmi o cataloghi presso il pubblico italiano (art. 7, co. 13 TUSMA).

In base alla suddetta norma, tali soggetti procedono alla sospensione della ricezione o ritrasmissione di SMA, nella misura loro possibile in base alle attività tecniche che svolgono, e comunque solo a seguito di un'intimazione di AGCOM e non autonomamente, quantomeno sulla base della disciplina applicabile ai SMA.

In sintesi, in Italia, uno di tali operatori può intervenire per bloccare la diffusione dei contenuti identificati dall'AGCOM, ma solo su richiesta di quest'ultima e non a propria discrezione, né in base a valutazioni autonome, nemmeno a seguito di contestazioni di terzi, fatti salvi gli obblighi applicabili ai fornitori di servizi di comunicazione elettronica¹⁴⁶.

141. Ai sensi del Codice europeo delle comunicazioni elettroniche approvato con d.lgs. 8 novembre 2021, n. 207 (come modificato con i «correttivi» di cui al d.lgs. 48/2024), le guide elettroniche ai programmi rientrano tra le «risorse correlate», e cioè tra i servizi correlati a una rete o a un servizio di comunicazione elettronica che permette o supporta la fornitura, l'auto fornitura o la fornitura automatizzata di servizi attraverso tale rete o servizio (art. 3, co. 1, lett. ccc). La nozione di «Electronic Program Guide» (EPG) non è specificamente definita dal suddetto Codice (né dalla direttiva UE 2018/1972, cit.). Dalla prassi si ricava che l'EPG può includere la lista dei canali e dei servizi a richiesta e cioè l'elenco numerico dei canali e servizi presenti sulla piattaforma televisiva e, ove disponibili, le informazioni dettagliate sui programmi di ciascun canale o servizio a richiesta. Su questi temi, v. da ultimo Regolamento AGCOM sulla definizione dell'icona per accedere ai canali della televisione digitale, approvato con Delibera 259/24/CONS.

142. Si pensi, ad esempio, ai canali in chiaro liberamente ricevibili con qualsiasi dispositivo di ricezione di segnali televisivi.

143. Sentenza Consiglio di Stato n. 04403/2024 cit. *supra* nota 138.

144. Per tali attività, v. le relative definizioni incluse nel TUSMA. Peraltro, va osservato che, in modo piuttosto «meccanico», nell'art. 7, co. 13 del TUSMA è stato inserito un riferimento alle PCV in occasione dell'attuazione della Direttiva SMA. Infatti, per le PCV, lo stesso TUSMA prevede l'applicazione delle norme di cui agli artt. 41 e 42.

145. Infatti, la piattaforma televisiva si avvale tipicamente dei servizi di terzi per organizzare la propria attività. Pertanto, le disposizioni dell'art. 7, comma 13, del TUSMA si applicano alla piattaforma televisiva solo nel caso in cui essa svolga direttamente una delle attività sopra indicate.

146. Infatti ai fornitori di servizi di comunicazioni si applicano anche le norme del DSA relative ai fornitori di servizi intermediari. Per quest'ultima definizione v. art. 3, par. 1, lett. g. e, per le norme del DSA loro applicabili, in particolare artt. 4-15.

Alla luce di quanto sopra, si può concludere che l'approccio regolamentare descritto ha permesso di preservare la distinzione dei ruoli, l'indipendenza e l'autonomia editoriale dei FSMA, tutelando al contempo il pluralismo dei media, senza impatti negativi sui cittadini e, più in generale, sul funzionamento del sistema democratico dei singoli Stati membri.

5. Analisi delle norme e dei loro rapporti

L'art. 18, par. 4, ult. co. dell'EMFA richiama espressamente gli artt. 28, 34, 35 del DSA e l'art. 28 *ter* della Direttiva SMA. Inoltre, l'art. 18, par. 4, ult. co. fa riferimento «agli obblighi relativi ai contenuti illegali che incombono loro in forza del diritto dell'Unione» senza riferirsi a una norma in particolare.

Ai fini di questa analisi, risulta importante non solo illustrare tali norme, ma anche analizzare il rapporto tra l'EMFA e il DSA, da un lato, e tra l'EMFA e la Direttiva SMA, dall'altro lato.

5.1. Gli artt. 28, 34 e 35 del DSA

L'art. 28 del DSA riguarda la 'Protezione online dei minori', imponendo alcuni obblighi a tutte le piattaforme online. In particolare, queste, se accessibili ai minori, devono adottare «misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione

dei minori sul loro servizio» e non devono mostrare «sulla loro interfaccia pubblicità basata sulla profilazione (...) se sono consapevoli, con ragionevole certezza, che il destinatario del servizio è un minore»¹⁴⁷.

Non viene specificato come tale tutela debba essere concretamente approntata, essendo «onere del singolo prestatore, fin dalla fase di creazione e progettazione del servizio, studiare e individuare misure adeguate e proporzionate al fine di garantire una reale ed effettiva protezione dei minori»¹⁴⁸. A tale proposito, «La Commissione, previa consultazione del comitato, può emanare orientamenti per assistere i fornitori di piattaforme online»¹⁴⁹.

Inoltre, secondo il considerando 89 del DSA, i VLOPP devono adottare misure atte a proteggere i minori dai contenuti che potrebbero nuocere al loro sviluppo fisico, mentale o morale, e fornire strumenti che consentano un accesso condizionato a tali informazioni¹⁵⁰.

Gli SMA e gli editori di pubblicazioni giornalistiche sono già soggetti a obblighi particolarmente stringenti in materia di tutela dei minori e rientrano nella sfera di vigilanza e nei poteri sanzionatori delle autorità e degli organismi competenti¹⁵¹.

Diventa allora difficile immaginare che tali operatori possano essere sottoposti a un vaglio discrezionale di soggetti privati (i VLOPP) con riguardo

147. L'art. 28 prevede nei suoi ultimi due commi quanto segue: «3. Il rispetto degli obblighi di cui al presente articolo non obbliga i fornitori di piattaforme online a trattare dati personali ulteriori per valutare se il destinatario del servizio sia minore. 4. La Commissione, previa consultazione del comitato, può emanare orientamenti per assistere i fornitori di piattaforme online nell'applicazione del paragrafo 1».

148. DE STEFANI 2023, che segnala che la previsione di cui all'art. 28 del DSA utilizza, con riguardo alle misure adeguate e proporzionate finalizzate a garantire un elevato livello di protezione dei minori, «una formulazione generica che lascia ampio margine di interpretazione» (p. 108).

149. Art. 28, par. 4 del DSA.

150. Il considerando 89 del DSA prevede in particolare che i VLOPP (e i fornitori di motori di ricerca di dimensioni molto grandi) «dovrebbero inoltre adottare misure atte a proteggere i minori dai contenuti che potrebbero nuocere al loro sviluppo fisico, mentale o morale e fornire strumenti che consentano un accesso condizionato a tali informazioni. Nel selezionare le misure di attenuazione appropriate, i fornitori possono tenere in considerazione, se del caso, le migliori pratiche del settore, comprese quelle stabilite attraverso la cooperazione in materia di autoregolamentazione, quali i codici di condotta, e dovrebbero tenere conto degli orientamenti della Commissione». Sulle «migliori pratiche», v. in Italia la coregolamentazione sugli accorgimenti tecnici applicabili ai SMA a richiesta, approvata con Delibera AGCOM 51/13/CSP; Delibera AGCOM 52/13/CSP di approvazione del regolamento in materia di criteri di classificazione delle trasmissioni televisive che possono nuocere gravemente allo sviluppo fisico, mentale o morale dei minori; Delibera AGCOM 9/23/CONS su Linee guida per i sistemi di controllo parentale (*parental control systems*) indirizzate agli operatori che forniscono servizi di comunicazione elettronica.

151. V. *supra* nota 13.

a compliance, peraltro di fonte unionale quanto ai SMA, già oggetto di specifica regolamentazione settoriale nei singoli Stati membri¹⁵².

Sembra quindi a chi scrive che, con riguardo ai MS, l'applicazione dell'art. 28 del DSA non possa prescindere quantomeno da una verifica di conformità alla disciplina settoriale (norme di legge, regolamentari, di autoregolamentazione e coregolamentazione) a tutela dei minori dello Stato membro con giurisdizione sugli stessi e, ove occorresse, da interlocuzioni con le autorità ed organismi nazionali competenti.

Peraltro, nel rapporto tra il DSA e la disciplina settoriale applicabile ai SMA, quest'ultima dovrebbe prevalere come previsto dallo stesso DSA (v. *infra* paragrafo 5.4.) e risulta dunque difficile prescindere dalla sua considerazione.

L'art. 34 del DSA disciplina la "Valutazione del rischio" che deve essere effettuata direttamente dai VLOPP e dai fornitori di motori di ricerca di dimensioni molto grandi (VLOSE – *Very Large Online Search Engines*)¹⁵³⁻¹⁵⁴.

Tale valutazione (cd. *risk assessment*) rappresenta uno dei primi adempimenti a carico dei VLOPP.

Infatti, entro quattro mesi dalla designazione di una VLOP, il fornitore di tale servizio deve svolgere il *risk assessment*¹⁵⁵, che consiste

nell'individuazione, analisi e valutazione dei "rischi sistemici", e cioè dei «rischi particolari che tali servizi di grandi dimensioni rappresentano per gli europei e la società»¹⁵⁶.

Successivamente, il *risk assessment* sarà effettuato una volta l'anno e «in ogni caso prima dell'introduzione di funzionalità che possono avere un impatto critico sui rischi individuati»¹⁵⁷.

La finalità della norma è di ridurre la portata dei «rischi sistemici», e cioè dei rischi intrinsecamente legati alla natura e al funzionamento dei servizi delle VLOP e che, in termini di portata ed effetti, possono avere un rilevante impatto sulla società¹⁵⁸.

Affinché tale valutazione non abbia effetti sproporzionati, i VLOPP sono tenuti non solo al rispetto di stringenti obblighi di diligenza, ma anche a porre in essere un'esecuzione efficace «al fine di individuare e attenuare adeguatamente i rischi e i danni sociali ed economici che possono verificarsi»¹⁵⁹.

Pertanto, tali soggetti sono tenuti a «valutare i rischi sistemici derivanti dalla progettazione, dal funzionamento e dall'uso dei loro servizi, nonché dai potenziali abusi da parte dei destinatari dei servizi» e ad «adottare opportune misure di attenuazione nel rispetto dei diritti fondamentali»,

152. V. norme sui SMA a tutela dei minori nella Direttiva SMA.

153. Si noti che gli artt. 34 e 35 si applicano anche ai fornitori di motori di ricerca di dimensioni molto grandi. Tuttavia, in questo contesto, il riferimento sarà ai VLOPP, poiché l'art. 18 dell'EMFA riguarda esclusivamente i fornitori di piattaforme online di dimensioni molto grandi. Sull'opportunità dell'estensione ai fornitori di motori di ricerca dell'art. 18 della Proposta di regolamento sulla libertà dei media (allora art. 17) si era soffermato l'ERGA, rilevando che «The category of very large online search engines as defined in the DSA should be part of the definitions alongside that of very large online platforms (article 2 (10)). It appears necessary to encompass these services, which play an important role in giving access to media content online and which therefore should be subject to the same, or at least similar, obligations as very large online platforms pursuant to EMFA articles 17 and 18.» (Proposal of the Commission for a European Media Freedom Act (EMFA), ERGA position, cit. nel commento all'art. Article 2 – Definizioni della Proposta di DSA, lett. C)).

154. Infatti, i rischi sistemici derivano dalla progettazione, funzionamento e uso dei servizi di intermediazione online e dai potenziali abusi dei destinatari degli stessi servizi. Pertanto, le piattaforme (e i motori di ricerca) di dimensioni molto grandi sono i soggetti ritenuti più adatti a valutarli.

155. Artt. 33, par. 6, co. 2 e 34, par. 1, co. 2 del DSA.

156. V. il [sito della Commissione europea](#).

157. Art. 34, par. 1., co. 2 del DSA.

158. Il DSA non fornisce una definizione espressa di "rischio sistemico". Anzi, i rischi sistemici vengono lasciati alla determinazione dei VLOPP (nonché dei motori di ricerca di dimensioni molto grandi).

159. Considerando 79 del DSA.

tenendo conto della «gravità dell'impatto potenziale e la probabilità» dei rischi sistemici¹⁶⁰.

In particolare, l'art. 34 prevede che i VLOPP devono individuare, analizzare e valutare «con diligenza gli eventuali rischi sistemici nell'Unione derivanti dalla progettazione o dal funzionamento del loro servizio e dei suoi relativi sistemi, compresi i sistemi algoritmici, o dall'uso dei loro servizi»¹⁶¹.

Il DSA non fornisce un elenco completo dei rischi sistemici. Infatti, esso prevede che la valutazione da parte dei fornitori di VLOP, in linea di principio, deve essere proporzionata alla gravità e probabilità dei rischi connessi ai loro servizi e deve includere almeno quattro categorie di rischi relativi:

- a) alla diffusione di contenuti illegali¹⁶²;
- b) agli eventuali effetti negativi per l'esercizio degli stessi diritti fondamentali¹⁶³;
- c) agli eventuali effetti negativi, attuali o prevedibili, sul dibattito civico, sui processi elettorali e sulla sicurezza pubblica;
- d) nonché agli effetti negativi, attuali o prevedibili, sulla violenza di genere, la protezione della salute pubblica e dei minori e le gravi

conseguenze negative per il benessere fisico e mentale della persona.

Per la valutazione dei rischi "sistemici", dovrà anche essere considerata l'eventualità e il modo in cui i seguenti fattori influenzano uno o più di tali rischi:

- i) la progettazione dei sistemi di raccomandazione e di qualsiasi altro sistema algoritmico pertinente;
- ii) i sistemi di moderazione dei contenuti;
- iii) le condizioni generali e la loro applicazione;
- iv) i sistemi di selezione e presentazione delle pubblicità;
- v) le pratiche del fornitore relative ai dati.

In aggiunta, occorre valutare «se e in che modo i rischi [...] siano influenzati dalla manipolazione intenzionale del loro servizio, anche mediante l'uso non autentico o lo sfruttamento automatizzato del servizio, nonché l'amplificazione e la diffusione potenzialmente rapida e ampia di contenuti illegali e di informazioni incompatibili con le condizioni generali.»¹⁶⁴.

L'art. 35 del DSA prevede che i rischi così individuati siano contrastati dai VLOPP con misure di attenuazione che siano ragionevoli, proporzionate

160. *Ibidem*.

161. Art. 34, par. 1 del DSA.

162. Considerando 80 del DSA che dispone che sono rischi associati alla diffusione di contenuti illegali ad esempio quelli relativi alla «diffusione di materiale pedopornografico o forme illegali di incitamento all'odio o altri tipi di abuso dei loro servizi per commettere reati, e lo svolgimento di attività illegali, quali la vendita di prodotti o servizi vietati dal diritto dell'Unione o nazionale, compresi i prodotti pericolosi o contraffatti e gli animali commercializzati illegalmente [...]. I fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi dovrebbero valutare il rischio di diffusione di contenuti illegali, indipendentemente dal fatto che le informazioni siano o meno incompatibili con le condizioni generali [...]». In questo contributo, argomento che le attività dei VLOPP, ai sensi degli artt. 34 e 35 del DSA, finalizzate a contrastare il rischio di diffusione di contenuti illegali, si distinguono da quelle relative all'esecuzione degli obblighi relativi ai contenuti illegali previsti nell'ultima parte dell'articolo 18, paragrafo 4, ultimo comma dell'EMFA, anche perché diversamente quest'ultima norma conterrebbe delle ripetizioni. V. a quest'ultimo riguardo *infra* paragrafo 5.3.

163. Più precisamente l'art. 34 del DSA fa riferimento agli «eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali, in particolare i diritti fondamentali alla dignità umana sancito nell'articolo 1 della Carta, al rispetto della vita privata e familiare sancito nell'articolo 7 della Carta, alla tutela dei dati personali sancito nell'articolo 8 della Carta, alla libertà di espressione e di informazione, inclusi la libertà e il pluralismo dei media, sanciti nell'articolo 11 della Carta, e alla non discriminazione sancito nell'articolo 21 della Carta, al rispetto dei diritti del minore sancito nell'articolo 24 della Carta, così come all'elevata tutela dei consumatori, sancito nell'articolo 38 della Carta» (par. 2, lett. b)).

164. Art. 34, par. 2, co. 2 del DSA.

ed efficaci, «prestando particolare attenzione agli effetti di tali misure sui diritti fondamentali»¹⁶⁵.

Pertanto, quest'ultima disposizione si raccorda con quella dell'art. 34 del DSA che prescrive che la valutazione dei rischi si estenda anche ai possibili impatti negativi che i servizi di intermediazione online possono produrre sulla libertà di espressione e sul pluralismo dei media (par. 1, lett. b).

Nonostante tali precisazioni, le modalità di implementazione degli artt. 34 e 35, che variano da VLOP a VLOP in base alla specificità di ciascun servizio, possono costituire un *vulnus* per la libertà e l'autonomia dei MSP, considerando l'ampia discrezionalità riconosciuta alle piattaforme online nell'esecuzione degli obblighi previsti da tali articoli¹⁶⁶.

In questa situazione, è auspicabile l'adozione di linee guida da parte della Commissione europea e di codici di condotta da parte dei soggetti interessati che supportino i VLOPP nella concreta individuazione dei rischi sistemici e delle misure di attenuazione dei rischi sistemici con particolare riferimento a soggetti qualificati come i MSP di cui all'art. 18, co. 1, dell'EMFA (artt. 35, par. 3 e 45, par. 2)¹⁶⁷.

In particolare, l'adozione di orientamenti da parte della Commissione europea, anche in collaborazione con i coordinatori dei servizi digitali, potrebbe quantomeno contribuire a fornire maggiore certezza nell'applicazione combinata delle norme dell'art. 18 dell'EMFA e del DSA, così come delle disposizioni della Direttiva SMA richiamate nel medesimo art. 18¹⁶⁸. Occorre, tuttavia, ricordare che si tratta di iniziative volontarie della Commissione e che gli orientamenti, una volta adottati, non sono vincolanti e non dovrebbero, a rigore, produrre effetti giuridici vincolanti¹⁶⁹.

Inoltre, come visto, con particolare riferimento al tema dell'eventuale inapplicabilità del *media privilege*, occorre valutare se i VLOPP, nell'esercizio della loro speciale responsabilità conformemente agli obblighi di diligenza previsti dal DSA, debbano comunque prevedere procedure specifiche più tutelanti per i contenuti dei SMA identificati con i loghi dei palinsesti o dei cataloghi autorizzati, o comunque soggetti a regolamentazione nei singoli Stati membri, e per quelli tratti da, o comunque collegati a, pubblicazioni di carattere giornalistico.

Infatti, da un lato, per i primi potrebbe sorgere un tema di inapplicabilità dell'art. 28 *ter* della Direttiva SMA; dall'altro lato, per entrambi potrebbe

165. Art. 35, par. 1 del DSA.

166. V. *supra* paragrafo 2.2.

167. Così NENADIC-BROGI 2024, «Under Article 35, the Board and the Commission collaborate to publish annual reports on systemic risks posed by large online platforms and search engines (their use or design). These reports are expected to detail risk identification, assessment, and mitigation guidelines and best practices considering both the national and Union-wide levels».

168. *Ibidem*, «The role of competent national authorities, through their EU platforms – the European Board for Digital Services and the European Board for Media Services, and their cooperation, will be essential in ensuring compliance and safeguarding fundamental rights». Le stesse Autrici rilevano, tuttavia, talune criticità per i diversi approcci che gli Stati membri potrebbero seguire nella determinazione dei propri coordinatori dei servizi digitali, soprattutto laddove questi ultimi soggetti non coincidano con le autorità dei media presenti nei singoli Stati membri.

169. Art. 28, par. 4 del DSA: «La Commissione, previa consultazione del comitato, può emanare orientamenti per assistere i fornitori di piattaforme online nell'applicazione del paragrafo 1.». Il relativo considerando 89 chiarisce che: «Nel selezionare le misure di attenuazione appropriate, i fornitori possono tenere in considerazione, se del caso, le migliori pratiche del settore, comprese quelle stabilite attraverso la cooperazione in materia di autoregolamentazione, quali i codici di condotta, e dovrebbero tenere conto degli orientamenti della Commissione»; art. 35, par. 3, del DSA «La Commissione, in cooperazione con i coordinatori dei servizi digitali, può emanare orientamenti sull'applicazione del paragrafo 1 in relazione a rischi concreti, con l'obiettivo specifico di presentare le migliori pratiche e raccomandare eventuali misure, tenendo debitamente conto delle possibili conseguenze di tali misure sui diritti fondamentali di tutte le parti interessate sanciti dalla Carta. Nell'elaborazione di tali orientamenti la Commissione organizza consultazioni pubbliche».

rendersi necessario ponderare attentamente l'inapplicabilità del *media privilege* con riguardo agli artt. 28, 34 e 35 del DSA¹⁷⁰.

Alla luce di quanto sopra, potrebbe farsi più pressante l'esigenza di un raccordo tra i VLOPP e i MSP con le Autorità europee e nazionali competenti.

5.2. L'art. 28 *ter* della Direttiva SMA

L'art. 28 *ter* della Direttiva SMA prevede che le Piattaforme di condivisione di Video (PCV) devono adottare "misure adeguate" per tutelare:

- i) i minori da programmi, video generati dagli utenti e comunicazioni commerciali che possano nuocere al loro sviluppo fisico, mentale o morale;
- ii) il grande pubblico da contenuti che istighino alla violenza o all'odio verso un gruppo di persone o un suo membro per uno dei motivi di cui all'art. 21 della Carta oppure che istighino a commettere reati di terrorismo, di pedopornografia ovvero di stampo razzista o xenofobo¹⁷¹.

Per le comunicazioni commerciali¹⁷², occorre distinguere tra quelle promosse, vendute o organizzate dalle stesse PCV e quelle che non ricadono sotto il controllo di queste ultime. Infatti, nel primo caso le PCV sono direttamente tenute al rispetto della normativa applicabile ai FSMA ai sensi dell'art. 9.1 della Direttiva SMA. Nel secondo caso, invece, le PCV devono adottare "misure adeguate".

Più in generale, la Direttiva SMA, in considerazione del limitato controllo che le PCV hanno sui contenuti presenti in rete, prevede il ricorso allo strumento delle "misure adeguate" per la tutela dei minori e del grande pubblico rispetto ai contenuti di cui sopra *sub* (i) e (ii).

Le PCV devono adottare misure adeguate destinate agli utenti attivi (e cioè gli utenti che "caricano" contenuti sulla piattaforma) e agli utenti "passivi" (cioè quelli che fruiscono dei contenuti in rete).

Quanto ai primi, viene ad esempio previsto l'obbligo per le PCV di inserire nelle condizioni generali il divieto di caricare contenuti illegali, nonché di rispettare le condizioni previste all'art. 9.1 della Direttiva SMA per le comunicazioni commerciali. A tal fine, le PCV devono adottare una funzionalità che consenta all'utente di dichiarare se il contenuto dallo stesso caricato contiene comunicazioni commerciali.

Quanto ai secondi, l'art. 28 *ter* prevede una serie di tutele, come ad esempio l'obbligo per le piattaforme online di segnalare la presenza di comunicazioni commerciali (per quelle caricate dagli utenti, nella misura in cui siano state da questi dichiarate), di istituire meccanismi di verifica dell'età degli utenti per i contenuti che possano nuocere ai minori (con divieto di utilizzare i dati dei minori così raccolti per fini commerciali, come il marketing diretto, la profilazione e la pubblicità mirata su base comportamentale), di dotarsi di sistemi di *parental control* sempre a tutela dei minori, nonché di strumenti efficienti di alfabetizzazione mediatica¹⁷³.

A tale riguardo, la coregolamentazione gioca un ruolo rilevante per le PCV poiché va a integrare il complessivo sistema normativo. In particolare, viene incoraggiata la coregolamentazione nazionale quale strumento di supporto alla migliore «*individuazione delle misure adeguate*»¹⁷⁴.

La valutazione dell'adeguatezza delle misure (e dunque anche degli strumenti a loro supporto)

170. V. *supra* paragrafo 3.

171. Art. 28 *ter*, par. 1 della Direttiva SMA. Su questo articolo, v. COLANTONI 2023, p. 995 ss.; GRANDINETTI 2022. Sul rapporto del DSA con la Direttiva SMA, v. FOLKERT-KALÉDA-LOWENTHAL 2024, p. 27.

172. Per la definizione di "comunicazioni commerciali", v. art. 1, par. 1, lett. h) della Direttiva SMA.

173. Art. 4 *bis* della Direttiva SMA. Sulla coregolamentazione v. CILIBERTI-SANFILIPPO 2024, pp. 57-102.

174. Per le piattaforme online soggette alla giurisdizione italiana, il nostro legislatore mantiene una posizione di apertura sia nei confronti delle procedure di coregolamentazione che nei confronti delle procedure di autoregolamentazione, lasciando ad AGCOM la scelta tra i due strumenti, sentito il Comitato di applicazione del Codice di autoregolamentazione *media e minori* V. a riguardo CILIBERTI-SANFILIPPO 2024, p. 57 ss.; MUSSELLI 2024, p. 103 ss.; POLLICINO-DE GREGORIO 2024, p. 249 ss., secondo i quali la disciplina delle piattaforme online ad opera del TUSMA rappresenta uno "step intermedio" nel contesto della regolamentazione dei servizi digitali (p. 255); DONATI 2019, che osserva che «l'autoregolamentazione e la coregolamentazione, pur rappresentando strumenti idonei a garantire la flessibilità indispensabile per il conseguimento degli obiettivi della direttiva

è affidata alle autorità o organismi nazionali di coregolamentazione. Infatti, ai sensi della Direttiva SMA, «Gli Stati membri si dotano dei meccanismi necessari per valutare l'adeguatezza delle misure [di cui al paragrafo 3] adottate dai fornitori di piattaforme per la condivisione di video. Gli Stati membri affidano la valutazione di tali misure alle autorità o agli organismi nazionali di regolamentazione.»¹⁷⁵.

In base alla normativa italiana di recepimento della Direttiva SMA, quale che sia lo strumento di soft regulation prescelto, i processi sono fortemente guidati dall'Autorità di regolamentazione che deve dettare apposite linee guida — sentiti l'Autorità garante per l'infanzia e l'adolescenza e il Comitato media e minori — tenendo conto di alcuni criteri indicati dalla normativa primaria, e cioè «(...) la natura e del contenuto del servizio offerto, del danno che questo può causare, delle caratteristiche della categoria di persone da tutelare nonché di tutti i diritti e gli interessi legittimi, compresi quelli dei fornitori della piattaforma per la condivisione di video e degli utenti che hanno creato o caricato contenuti, nonché dell'interesse pubblico generale), fermo restando che non potrà chiedere alle PCV di adottare misure che mirino al controllo preventivo/filtraggio dei contenuti quando sono caricati né misure che non siano praticabili/proporzionate»¹⁷⁶.

Pertanto, risulta evidente la differenza tra le norme del DSA e quelle della Direttiva SMA. Infatti, le norme di cui all'art. 28 *ter* della Direttiva SMA, seppure ampie per taluni aspetti (la nozione di "misure adeguate" potrebbe apparire di difficile perimetrazione), prevedono comunque un controllo *ex ante* dell'adeguatezza delle misure da parte delle autorità nazionali e degli organismi di coregolamentazione.

Le PCV dovranno dunque conformarsi alle linee guida di AGCOM nell'adozione dei propri codici di condotta.

In particolare, devono essere comunicati ad AGCOM codici di autoregolamentazione o di coregolamentazione a seconda delle determinazioni di quest'ultima, che ne verifica la conformità alla normativa primaria e ai propri regolamenti, attribuendo loro efficacia con delibera di approvazione e vigilando sulla loro attuazione¹⁷⁷.

Compete ad AGCOM stabilire la procedura di vigilanza concernente il monitoraggio e la valutazione periodica di conformità, nel rispetto dei principi di trasparenza, non discriminazione e proporzionalità¹⁷⁸.

Alla luce di quanto sopra, ci si chiede come operi il richiamo all'art. 28 *ter* della Direttiva SMA contenuto nell'art. 18 dell'EMFA. Infatti, quest'ultimo articolo non riguarda qualsiasi PCV, ma solo quelle qualificabili come VLOP.

Inoltre, come visto, l'art. 28 *ter* della Direttiva SMA prevede che il controllo dell'adeguatezza delle misure adottate dalle PCV sia verificato dalle autorità o organismi pertinenti nazionali, mentre l'art. 18 dell'EMFA non prevede un controllo preventivo, da parte della Commissione europea o di altri organi, delle misure che i VLOPP intendono adottare.

L'art. 28 *ter* riguarda le PCV, e cioè una *species* all'interno del più ampio genere delle piattaforme online. In quanto norma settoriale, l'art. 28 *ter* dovrebbe prevalere, in via di principio, sul DSA, almeno per quanto riguarda le PCV che si qualificano anche come VLOP. Inoltre, le PCV sono soggette alla giurisdizione dello Stato membro competente, mentre i VLOPP sono sottoposti ai poteri esclusivi della Commissione europea, limitatamente alla vigilanza e all'applicazione del capo III, sezione 5, del DSA; cioè in relazione agli obblighi supplementari previsti, tra i quali quelli di cui agli artt. 34 e 35 sopra esaminati¹⁷⁹.

Ai fini dell'applicazione dell'art. 28 *ter* della Direttiva SMA, come richiamato all'art. 18, par. 4, ult. co., dell'EMFA, sembra dunque che la prima

2010/13/UE, dovranno mantenersi nell'ambito dei principi che il legislatore nazionale è comunque chiamato a definire» (p. 72).

175. Articolo 28 *bis*, par. 5 della Direttiva SMA.

176. Art. 42, co. 5 del TUSMA.

177. Art. 42, co. 3 del TUSMA.

178. Art. 42, co. 5 del TUSMA.

179. V. *supra* paragrafo 5.1. Sui poteri della Commissione europea con riguardo ai VLOPP, v. FOLKERT-KALÉDA-LOWENTHAL 2024, p. 375 ss.; AA.VV. 2023, p. 203 ss.

norma debba rimanere nel suo contesto originario, con la vigilanza e i poteri sanzionatori riservati alle Autorità e organismi nazionali competenti.

Alla luce di quanto sopra, pare ragionevole ritenere che il richiamo all'art. 28 *ter* contenuto nell'art. 18 dell'EMFA sia indirizzato solo ai VLOPP che rientrano anche nella nozione di fornitore di una PCV. Pertanto, le norme dell'art. 28 *ter*, come trasposte nei singoli ordinamenti degli Stati membri, dovrebbero applicarsi ai suddetti VLOPP solo ai fini dell'art. 18, par. 4, ult. co. dell'EMFA.

In tal senso, nonostante la complessità derivante da tale sovrapposizione di soggetti e obblighi, si potrebbe concludere che l'art. 18, par. 4, ult. co., dell'EMFA si riferisca alle "misure adeguate" che i fornitori di PCV/VLOP sono tenuti ad adottare ai sensi delle singole normative nazionali di attuazione della Direttiva SMA.

Tuttavia, anche queste misure, sebbene siano soggette al controllo delle autorità e degli organismi nazionali competenti, non appaiono sufficientemente certe.

Infine, riguardo ai SMA si pone una questione ancora più fondamentale, poiché la Direttiva SMA li disciplina con un apparato di norme anche più stringente rispetto a quello previsto all'art. 28 *ter*, indipendentemente dalla modalità o dal mezzo di diffusione. Come si illustrerà al successivo paragrafo 5.5, l'art. 28 *ter* non sembra, infatti, estensibile a qualsiasi contenuto diffuso da uno SMA.

5.3. Gli obblighi relativi ai contenuti illegali

Il riferimento ai "contenuti illegali" di cui all'art. 18, par. 4, co. ult. dell'EMFA appare finalizzato a coprire ogni fattispecie residuale, ma solo limitatamente agli «obblighi relativi ai contenuti illegali che incombono» sui VLOPP «in forza del diritto dell'Unione».

Il DSA definisce, all'art. 3, par. 1, lett. h), il contenuto illegale come «qualsiasi informazione che, di per sé o in relazione a un'attività, tra cui

la vendita di prodotti o la prestazione di servizi, non è conforme al diritto dell'Unione o di qualunque Stato membro conforme con il diritto dell'Unione, indipendentemente dalla natura o dall'oggetto specifico di tale diritto» e chiarisce che «il concetto di "contenuto illegale" dovrebbe essere definito in senso lato per coprire anche le informazioni riguardanti i contenuti, i prodotti, i servizi e le attività illegali. Tale concetto dovrebbe, in particolare, intendersi riferito alle informazioni, indipendentemente dalla loro forma, che ai sensi del diritto applicabile sono di per sé illegali, quali l'illecito incitamento all'odio o i contenuti terroristici illegali e i contenuti discriminatori illegali, o che le norme applicabili rendono illegali in considerazione del fatto che riguardano attività illegali. Tra queste figurano, a titolo illustrativo, la condivisione di immagini che ritraggono abusi sessuali su minori, la condivisione non consensuale illegale di immagini private, il cyberstalking (pedinamento informatico), la vendita di prodotti non conformi o contraffatti, la vendita di prodotti o la prestazione di servizi in violazione della normativa sulla tutela dei consumatori, l'utilizzo non autorizzato di materiale protetto dal diritto d'autore, l'offerta illegale di servizi ricettivi o la vendita illegale di animali vivi. [...] A tale riguardo è irrilevante che l'illegalità delle informazioni o delle attività sia sancita dal diritto dell'Unione o dal diritto nazionale conforme al diritto dell'Unione e quale sia la natura esatta o l'oggetto preciso della legge in questione.»¹⁸⁰.

Tra gli obblighi gravanti sui VLOPP in merito ai contenuti illegali, vi sono quelli di cui agli artt. 9, 10, 16 e 22 del DSA, che riguardano l'ottemperanza agli ordini di contrasto dei contenuti illegali e di fornitura di informazioni, i meccanismi di segnalazione e azione, nonché i segnalatori attendibili di contenuti illegali.

Le regole procedurali che assistono tali fattispecie appaiono garantire sufficientemente i diritti

180. Considerando 12 del DSA. Sui contenuti illegali v. anche considerando 37, 38, 157. Critica la chiarezza della nozione di contenuti illegali della Proposta di DSA per come "calata" nell'art. 14 (Meccanismo di notifica e azione), poi art. 16 del DSA, BARATA 2021, p. 15 ss. Il DSA infine approvato ha aggiunto delle precisazioni ai testi normativi, prevedendo che la segnalazione dei contenuti da parte di qualsiasi persona o enti rechi una «spiegazione sufficientemente motivata dei motivi per cui [...] presume che le informazioni in questione costituiscano contenuti illegali». Per un'analisi della nozione di "contenuti illegali" nell'art. 26 (valutazione del rischio) della Proposta di DSA (poi art. 34 del DSA), *Ibidem*, 17. V. anche FOLKERT-KALÉDA-LOWENTHAL 2024, pp. 38-39; TOMMASI 2023, p. 17 ss.; MCHANGAMA-ALKIVIADOU-MENDIRATTA 2022. Sui contenuti illegali, v. anche *supra* note 36-40 e paragrafo 3.

fondamentali dei MSP. In particolare, le fattispecie che, ai sensi del diritto applicabile, sono illegali non paiono porre particolari questioni per i fornitori di MS quando sono oggetto di ordini o di segnalazione da parte di soggetti qualificati.

Inoltre, tra gli ulteriori obblighi “relativi ai contenuti illegali”, vi sono ad esempio quelli di cui all’art. 17 della Direttiva DSM. Un VLOPP che dovesse agire a tutela della proprietà intellettuale non sarebbe astrattamente tenuto ad osservare il *media privilege*, anche perché in tal caso dovrebbero prevalere le procedure previste dalla Direttiva DSM e dai conseguenti interventi normativi della Commissione europea e delle Autorità nazionali, a meno di non ricadere nella gestione dei rischi cd. sistemici¹⁸¹.

Come visto, l’art. 17 della Direttiva DSM non pone specifici problemi dal momento che, come precisato dalla Corte di Giustizia, gli interventi posti in essere ai sensi di tale Direttiva devono essere “rigorosamente mirati” nel senso che devono riguardare i contenuti illeciti e non avere un effetto arbitrario o eccessivo sui contenuti leciti¹⁸².

Inoltre, sempre a titolo esemplificativo, rileva il Regolamento europeo sul contrasto della diffusione online di contenuti terroristici che prevede l’obbligo dei prestatori di servizi di ottemperare agli ordini di «rimuovere contenuti terroristici o di disabilitare l’accesso a contenuti terroristici» (art. 3).

In ogni caso, eventuali criticità riguardo all’applicazione del *media privilege* potrebbero essere superate, come già evidenziato, da un coordinamento con le Autorità o gli organismi competenti

a vigilare sui MSP o dall’adozione di orientamenti ad opera della Commissione europea¹⁸³.

5.4. Il rapporto tra DSA e EMFA

Il DSA dispone che esso non prevale su altri atti del diritto dell’Unione che:

- a) disciplinano in generale la prestazione di servizi della società dell’informazione (come ad esempio quelli relativi alla tutela dei consumatori, alla protezione dei dati personali, ai diritti di proprietà intellettuale) e su quelli che
- b) regolano altri aspetti della prestazione di servizi intermediari nel mercato interno o specificano e integrano le norme armonizzate dallo stesso Regolamento DSA, come ad esempio la Direttiva SMA che, si ricorda, viene integrata dal Regolamento EMFA.

Pertanto, da un lato, le norme di carattere generale o orizzontali dovrebbero prevalere sul Regolamento DSA; dall’altro, il Regolamento DSA dovrebbe prevalere su aspetti non affrontati o solo parzialmente trattati da altri atti settoriali dell’Unione europea¹⁸⁴.

Inoltre, il Regolamento DSA interviene sulle questioni per le quali tali altri atti giuridici lasciano agli Stati membri la facoltà di adottare determinate misure a livello nazionale¹⁸⁵.

L’EMFA è considerata una normativa speciale non solo perché integra la normativa settoriale della Direttiva SMA, ma anche perché disciplina aspetti specifici rispetto a quelli più generali trattati dal Regolamento DSA, in particolare per quanto riguarda la libertà dei media¹⁸⁶.

Ciò premesso, è pur vero che è lo stesso Regolamento EMFA a richiamare le norme del

181. Art. 28 *ter*, par. 5 della Direttiva SMA.

182. V. anche art. 1, par. 2 dell’EMFA.

183. Questa conclusione è stata già ribadita *supra* paragrafi 1, 2.1., 2.2., 3 e *infra* nel paragrafo 6.

184. Art. 2.4., nonché considerando 10 del DSA che così chiarisce: «Il presente regolamento non dovrebbe pregiudicare altri atti del diritto dell’Unione che disciplinano la prestazione di servizi della società dell’informazione in generale, che disciplinano altri aspetti della prestazione di servizi intermediari nel mercato interno o che specificano e integrano le norme armonizzate di cui al presente regolamento».

185. Secondo il considerando 10 del DSA «nella misura in cui tali atti giuridici dell’Unione perseguono gli stessi obiettivi del presente regolamento, le norme del presente regolamento si dovrebbero applicare in relazione alle questioni che non sono affrontate o non sono pienamente affrontate da tali altri atti giuridici nonché alle questioni sulle quali tali altri atti giuridici lasciano agli Stati membri la facoltà di adottare determinate misure a livello nazionale.».

186. Sulla natura di *lex specialis* del Regolamento EMFA, v. MASSA 2024, p. 314.

Regolamento DSA al suo art. 18, par. 4, ult. co., precisamente con riguardo al meccanismo del *media privilege*.

Tuttavia, come visto, nel rapporto tra norma speciale e norma generale, la prima dovrebbe giocare un ruolo rilevante rispetto alla seconda. Infatti, anche laddove la norma generale intervenga ad integrare quella speciale, secondo quanto esposto, tale integrazione dovrebbe avvenire in modo da risultare coerente con gli obiettivi della normativa speciale.

Come visto, l'art. 28 del DSA disciplina la protezione online dei minori imponendo alle piattaforme online l'adozione di misure adeguate e proporzionate per assicurare sui loro servizi un elevato livello di tutela della vita privata, della sicurezza e della protezione dei minori. L'art. 34 del DSA impone alle piattaforme online di grandi dimensioni di individuare e valutare, nel rispetto di specifiche tempistiche, gli eventuali rischi sistemici derivanti dai loro servizi relativamente alla diffusione di contenuti illegali e agli effetti negativi di tali rischi sull'esercizio dei diritti fondamentali, sul dibattito civico, sui processi elettorali, sulla sicurezza pubblica, nonché in relazione alla violenza di genere, alla salute pubblica e dei minori o al benessere fisico o mentale della persona. L'art. 35 del DSA regola l'obbligo a carico delle piattaforme online di grandi dimensioni di adottare misure di attenuazione dei rischi sistemici, quali individuati ai sensi dell'art. 34. L'art. 35 elenca a riguardo una serie di possibili misure relative, ad esempio, all'adeguamento dei servizi, delle condizioni generali e della loro applicazione o delle procedure di moderazione¹⁸⁷, all'aggiornamento delle loro interfacce o all'adozione di misure mirate a tutela dei minori,

oppure l'adozione sulle loro interfacce di contrasti per identificare contenuti manipolati o falsamente autentici.

Sulla base di tali norme, un MS potrebbe essere oggetto di limitazione, in tutto o anche solo per specifici suoi contenuti, senza previo contraddittorio, nel caso in cui sia necessario tutelare i minori o per dare applicazione alle misure predisposte al fine di fare fronte ai rischi sistemici o, ancora, per adempiere agli obblighi, a carico dei VLOPP, con riguardo a contenuti illegali.

Tuttavia, come visto, lo stesso Regolamento DSA stabilisce la sua prevalenza rispetto alle discipline settoriali eventualmente applicabili solo per gli aspetti che non sono trattati o non sono pienamente affrontati dalle seconde.

Se ne deduce che, quantomeno agli SMA, dovrebbero applicarsi in primo luogo le norme della Direttiva SMA rispetto a quelle del Regolamento DSA.

Tali normative coprono oggi diversi ambiti e in particolare la tutela dei minori e del grande pubblico nei settori coordinati dalla Direttiva SMA.

In aggiunta a quanto sopra, occorre anche considerare che i SMA sono soggetti a norme ulteriori rispetto a quelle derivanti dalla Direttiva SMA, come ad esempio quelle in materia di par condicio. A questo riguardo, nella Comunicazione della Commissione COM(2018) 236 def., si riconosce che «In Europa, i media tradizionali sono già soggetti ad un'ampia gamma di norme in materia di imparzialità, pluralismo, diversità culturale, contenuti dannosi, pubblicità e contenuti sponsorizzati. La democrazia nell'Unione europea si basa sull'esistenza di media liberi e indipendenti»¹⁸⁸.

187. Sulle attività di moderazione v. *supra* nota 40.

188. Si tratta della Comunicazione «Contrastare la disinformazione online: un approccio europeo». A questa Comunicazione si è aggiunta la Comunicazione *Orientamenti della Commissione per i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi sull'attenuazione dei rischi sistemici per i processi elettorali a norma dell'articolo 35, paragrafo 3, del regolamento (UE) 2022/2065 (C/2024/3014)*. Inoltre, il 14 marzo 2024 è stato adottato un Regolamento europeo *2024/900* relativo alla trasparenza e al targeting della pubblicità politica. L'obiettivo è garantire che i messaggi di pubblicità politica siano facilmente riconoscibili, identificare il committente e verificare se siano indirizzati esclusivamente a una persona o a un gruppo specifico di persone (o se escludano tale persona o gruppo) sulla base del trattamento di dati personali. Questo, al fine di contrastare la manipolazione delle informazioni e le ingerenze straniere nelle elezioni, assicurando ai cittadini la possibilità di compiere scelte informate. Il 26 aprile 2024 la Commissione europea ha pubblicato gli Orientamenti per i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi sull'attenuazione dei rischi sistemici per i processi elettorali a norma dell'articolo 35, paragrafo 3, del DSA (Comunicazione della Commissione *Orientamenti*

5.5. La Direttiva SMA e l'EMFA

Con riguardo al rapporto tra EMFA e Direttiva SMA, ed in particolare con riguardo all'art. 28 *ter* di quest'ultima la questione non è tanto di definizione della natura delle due normative, entrambi speciali, quanto piuttosto dello stesso assoggettamento dei MSP, e in particolare dei FSMA, a tale norma della Direttiva SMA.

Quest'ultima Direttiva prevede, nel suo considerando 3, ult. periodo, con riguardo ai SMA diffusi attraverso piattaforme on line di condivisione di video, che: «I canali o altri servizi audiovisivi sotto la responsabilità editoriale di un fornitore possono essi stessi costituire servizi di media audiovisivi, anche se sono offerti su una piattaforma per la condivisione di video caratterizzata dall'assenza di responsabilità editoriale. In questi casi spetterà ai fornitori la responsabilità editoriale di conformarsi alla direttiva 2010/13/UE».

Questa disposizione evidenzia, da un lato, che il fornitore di una PCV non è considerato tale riguardo a uno SMA dallo stesso edito (essendo piuttosto, per questo aspetto, un FSMA e, in quanto tale, soggetto alle norme della Direttiva SMA). Dall'altro lato (e questo è l'aspetto che qui rileva), in relazione ad uno SMA di un editore terzo presente su una PCV, il fornitore di tale piattaforma non dovrebbe avere obblighi a suo carico, ai sensi della Direttiva SMA né tantomeno dovrebbe esercitare conseguenti prerogative.

Infatti, l'editore di uno SMA, che è autonomamente responsabile del proprio servizio, è già destinatario di obblighi ai sensi della Direttiva SMA, talvolta più restrittivi, ed è soggetto alla vigilanza e alla potestà sanzionatoria delle Autorità regolamentari competenti nei singoli Stati membri (AGCOM in Italia).

Un doppio controllo, ai sensi della Direttiva SMA, da parte delle piattaforme online e delle Autorità per l'osservanza di analoghi obblighi, non appare né ragionevole né proporzionato.

Ne consegue che, come emerge anche dal considerando 3 succitato della Direttiva SMA, i FSMA presenti su una piattaforma online sono tenuti a rispettare le norme loro direttamente applicabili ai sensi della Direttiva SMA, mentre le piattaforme online non dovrebbero avere una responsabilità ai sensi dell'art. 28 *ter* sui contenuti diffusi dai FSMA attraverso le VLOP¹⁸⁹.

Naturalmente, dovrebbe trattarsi di contenuti tratti da uno SMA autorizzato o comunque soggetti a regolamentazione ai sensi della normativa settoriale applicabile nel singolo Stato membro¹⁹⁰.

6. La speciale responsabilità dei fornitori di VLOP

Alla luce dell'analisi svolta risulta piuttosto evidente che il rispetto delle garanzie espressamente previste per i MSP dalla CEDU e dalla Carta, nonché l'esistenza nei singoli Stati membri di un complesso di norme che regolamentano i MSP, pongono

della Commissione per i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi sull'attenuazione dei rischi sistemici per i processi elettorali a norma dell'articolo 35, paragrafo 3, del Regolamento (UE) 2022/2065 (OJ C, C/2024/3014, 26.04.2024). Secondo tale Raccomandazione, «I giornalisti e i fornitori di servizi di media svolgono un ruolo fondamentale nella raccolta, nel trattamento e nella comunicazione di informazioni al pubblico, ruolo che diviene ancora più cruciale durante i periodi elettorali. Le organizzazioni e i fornitori di servizi di informazione indipendenti con norme e procedure editoriali interne consolidate sono ampiamente considerati fonti di informazione affidabili. I fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi dovrebbero pertanto collaborare con le organizzazioni dei media indipendenti, le autorità di regolamentazione, la società civile e le organizzazioni di base, i verificatori di fatti, il mondo accademico e altri portatori di interessi pertinenti su iniziative volte a migliorare l'individuazione di informazioni affidabili e la possibilità per gli utenti di accedere a contenuti mediatici informativi pluralistici relativi alle elezioni, provenienti da fonti affidabili» (par. 49). Il rapporto tra fornitori di SMA e piattaforme online risulta qui quasi rovesciato dal momento che sono le seconde che dovrebbero apprendere dai primi metodologie e procedure per migliorare le informazioni affidabili soprattutto in periodi particolarmente sensibili per la salvaguardia della democrazia degli Stati membri, come quelli elettorali.

189. GRANDINETTI 2022-B, p. 105 ss.

190. V. *supra* paragrafi 3 e 5.1.

rilevanti questioni in merito all'attribuzione di potestà di fatto regolamentari in capo ai VLOPP. Infatti, questa sorta di delega di poteri risulta *prima facie* inconciliabile con tale assetto o comunque problematica¹⁹¹.

In questa situazione, assume rilevanza la speciale responsabilità dei VLOPP nella sospensione o limitazione della visione di contenuti informativi, la quale richiede, quantomeno, una conoscenza approfondita del complesso di norme applicabili ai MSP nei singoli Stati membri e della relativa prassi amministrativa.

Tuttavia, anche questo approccio comporta indirettamente il riconoscimento di un trasferimento di "competenze" dalle Autorità e organismi preposti alla vigilanza delle attività dei MSP a soggetti privati.

L'adozione da parte della Commissione europea, in collaborazione con i coordinatori dei servizi digitali, di orientamenti sull'applicazione degli artt. 28, 34 e 35 del DSA e dell'art. 28 *ter* della Direttiva SMA, nonché più in generale relativamente all'intervento dei VLOPP in caso di contenuti illegali, potrebbe rappresentare la soluzione più adeguata per mitigare il rischio di una completa delega di poteri a favore dei VLOPP nei confronti dei MSP.

In ogni caso, tali interventi potrebbero contribuire a superare una serie di dubbi interpretativi e applicativi, quali quelli illustrati in questo contributo.

Infatti, nonostante gli orientamenti siano solo volontari e privi di effetto giuridico, la Commissione europea potrebbe comunque fornire indicazioni ai VLOPP per l'implementazione degli obblighi previsti dal DSA e dall'EMFA nei confronti dei MSP, garantendo così una migliore tutela dei diritti fondamentali di questi ultimi rispetto all'ampia discrezionalità che i testi normativi lasciano ai VLOPP.

In questo quadro, assumono particolare rilevanza anche le norme di cui all'art. 18 dell'EMFA, già evidenziate sopra¹⁹², che prevedono:

- a) l'obbligo dei fornitori di VLOP di «avviare un dialogo significativo ed efficace con il fornitore di servizi di media, su sua richiesta, in buona fede, al fine di trovare una soluzione amichevole,

entro un lasso di tempo ragionevole, per porre fine alle restrizioni o sospensioni ingiustificate ed evitarle in futuro» (par. 6),

- b) la facoltà per il MSP di notificare l'esito e i dettagli di tale dialogo al Consiglio e alla Commissione e di richiedere al Consiglio di «emettere un parere sull'esito di tale dialogo, comprese, ove pertinenti, le azioni raccomandate» al fornitore di VLOP» (par. 6),
- c) l'obbligo del fornitore di VLOP di pubblicare su base annua informazioni dettagliate su:
 - i) il numero di casi in cui ha imposto restrizioni o sospensioni sulla base del fatto che il contenuto fornito da un MSP "qualificato" è risultato incompatibile con i suoi termini e condizioni;
 - ii) i motivi per l'imposizione di tali restrizioni o sospensioni, comprese le clausole specifiche dei termini e delle condizioni con cui il contenuto del MSP è stato ritenuto incompatibile;
 - iii) il numero di dialoghi intercorsi con i fornitori di servizi di media;
 - iv) il numero di casi in cui ha respinto dichiarazioni presentate da un fornitore di servizi di media e i motivi del rigetto;
 - v) il numero di casi in cui ha invalidato una dichiarazione presentata da un fornitore di servizi di media ai sensi del paragrafo 1 e i motivi di invalidazione (par. 8);
 - vi) l'emanazione da parte della Commissione di orientamenti «al fine di agevolare l'attuazione coerente ed efficace del presente articolo» (par. 9).

7. Conclusioni

Dall'analisi svolta emerge che il *media privilege*, come disciplinato dall'EMFA, non rappresenta la soluzione definitiva per meglio regolamentare il rapporto tra MSP e VLOPP.

Infatti, il *media privilege* è solo un primo passo per rafforzare la natura speciale dei MSP quali fattori di democrazia dell'Unione europea.

La soluzione potrebbe, infatti, risiedere nella modifica delle procedure esistenti nei singoli Stati membri relativamente alla vigilanza e

191. Sul tema della delega di poteri ai fornitori di VLOP, v. GRANDINETTI 2022-B; DE GREGORIO 2019. V. anche note 81-97.

192. V. *supra* paragrafo 2.1.

all'applicazione delle sanzioni ai MSP per i contenuti diffusi online, quando violano normative settoriali. Ancora oggi, infatti, le procedure sono le stesse sia per l'ambiente online sia per quello offline. D'altro canto, se non si andasse in questa direzione, l'evoluzione delle tecnologie e delle modalità distributive dei contenuti potrebbe portare alla definitiva perdita di poteri in capo alle autorità nazionali legittimate democraticamente¹⁹³.

Medio tempore, occorrerebbe monitorare attentamente le condotte dei VLOPP per verificare che i loro interventi nei confronti dei MSP avvengano nel rispetto dei diritti fondamentali riconosciuti dalla Carta.

Inoltre, considerato il rapporto di specialità tra EMFA e DSA, il primo dovrebbe astrattamente prevalere sul secondo o, quantomeno, dovrebbe essere favorita un'interpretazione delle norme rilevanti secondo la quale gli obiettivi dell'EMFA, e cioè l'indipendenza e l'autonomia dei MSP, rappresentino principi guida nell'applicazione del DSA e siano, quindi, particolarmente considerati nell'applicazione degli artt. 28, 34 e 35 del DSA.

Infatti, risulta evidente che il corretto coordinamento delle norme di cui al Regolamento DSA e di quelle di cui all'EMFA sia fondamentale al fine di non creare contraddizioni interne al sistema e per prevenire possibili contrasti con l'art. 11 della Carta anche alla luce degli orientamenti della Corte di Giustizia, nonché con l'art. 10 della CEDU come interpretato dalla Corte EDU.

Analoghe considerazioni valgono per le disposizioni della Direttiva SMA relative alle piattaforme di condivisione video richiamate nell'ultimo capoverso dell'art. 18 dell'EMFA (e cioè l'art. 28 *ter* della Direttiva SMA).

Dall'analisi svolta emerge anche l'importanza di un'interpretazione restrittiva delle deroghe previste dall'art. 18, par. 4, ult. co. dell'EMFA, in modo da evitare derive che possano rappresentare un danno irrimediabile per i diritti fondamentali dei MSP qualificati.

In tal senso occorre valutare attentamente l'inapplicabilità del *media privilege* di cui all'art. 18,

par. 4, ult. co. dell'EMFA ai contenuti riconducibili a un MS che sia già oggetto di regolamentazione da parte delle Autorità o degli organismi del singolo Stato membro di appartenenza di quest'ultimo. Come visto, tali contenuti potrebbero facilmente distinguersi dagli altri dello stesso MSP diffusi online grazie ad un logo o ad una dicitura che identifichi il SMA o la pubblicazione di carattere giornalistico da cui gli stessi siano stati tratti o alla quale siano comunque collegati.

Infatti, in un'ottica di applicazione restrittiva delle deroghe, si potrebbe valutare se l'inapplicabilità del *media privilege* debba riguardare solo i contenuti che, pur riconducibili a un MSP qualificato, sfuggano a regolamentazione sulla base della disciplina applicabile nel singolo Stato membro di appartenenza o che non ricadano nella nozione di "pubblicazione di carattere giornalistico".

Inoltre, secondo l'interpretazione proposta delle norme, i contenuti degli MSP qualificati che siano già soggetti a regolamentazione settoriale, o che rientrino nella nozione di "pubblicazione di carattere giornalistico", sarebbero comunque sottoposti alle attività di moderazione dei VLOPP ai sensi dell'art. 18 dell'EMFA, ma beneficerebbero di un previo contraddittorio con questi ultimi prima che i loro contenuti possano essere sospesi o limitati.

In ogni caso, in base ad un'applicazione coordinata degli artt. 28, 34 e 35 del DSA e dell'art. 18, par. 4, ult. co. dell'EMFA, i VLOPP dovrebbero considerare la particolare natura dei media qualificati ai sensi del par. 1 dell'art. 18 dell'EMFA e la necessità, ribadita più volte nel DSA, di «prestare particolare attenzione agli effetti di tali misure sui diritti fondamentali»¹⁹⁴.

In quest'ottica, anche al fine di «beneficiare dei vantaggi di un mercato integrato e sviluppato»¹⁹⁵ e considerando che le norme vigenti lo permettono, sarebbe auspicabile una perimetrazione veloce e prevedibile delle attività di moderazione dei VLOPP nei confronti dei MSP qualificati, oltre che dell'applicazione della deroga prevista dall'art. 18, par. 4, ult. co., che potrebbe essere raggiunta grazie a un dialogo costruttivo e al coordinamento tra

193. V. a riguardo HUSOVEC 2024, secondo il quale «Through the DSA, parliaments can better learn and improve the content rules too. However, it is them who need to take the action. In liberal democracies, parliaments have the legitimacy to make content rules and are accountable to the judiciary and the public» (p. 54). V. *infra* nota 197.

194. Ad es. agli artt. 1, 14, par. 4, 34, par. 1, co. 1, lett. b), 35, parr. 1 e 3 del DSA.

195. Considerando 14 dell'EMFA.

il Consiglio, il Comitato, i coordinatori dei servizi digitali¹⁹⁶ e la Commissione europea¹⁹⁷.

Anche il coordinamento tra soggetti privati (VLOPP e MSP) e Autorità competenti, europee e nazionali, potrebbe favorire il rafforzamento della tutela dei diritti in campo, come ribadito dall'Assemblea parlamentare del Consiglio d'Europa affermando che «Moreover, stronger collaboration between public authorities and the private sector is required»¹⁹⁸.

Infine, l'adozione di codici di condotta europei, elaborati dalle piattaforme online con le pertinenti autorità, le organizzazioni della società civile e altre parti interessate, ed in particolare i MSP, sotto la supervisione della Commissione europea¹⁹⁹, potrebbe contribuire alla effettiva tutela dei diritti fondamentali in campo.

196. Anche la cooperazione tra coordinatori dei servizi digitali (considerando 127-137 del DSA), nonché di questi con la Commissione europea, riveste una particolare importanza per le finalità illustrate (v. Capo IV del DSA). V. anche considerando 10 della Raccomandazione della Commissione [C\(2023\) 7170](#) final sul coordinamento delle risposte agli incidenti, cit., che incoraggia gli Stati membri, nelle more della piena applicazione del DSA, «ad assistere la Commissione nel suo compito di monitoraggio e applicazione del regolamento (UE) 2022/2065 in relazione alle piattaforme online di dimensioni molto grandi designate e ai motori di ricerca online di dimensioni molto grandi designati». Inoltre, la Raccomandazione sottolinea che: «(...) è auspicabile che gli Stati membri agiscano in modo coordinato a sostegno delle eventuali azioni di esecuzione che la Commissione può adottare nell'esercizio dei suoi poteri di cui al capo IV, sezione 4, del regolamento (UE) 2022/2065.» (considerando 15). Sulla rilevanza di un coordinamento istituzionale v. anche Broughton Micova-Schnurr-Calee-Enstone 2024, «An inclusive, cooperative process should take place, possibly led by the Digital Services Board and the Commission to set priorities among the risk areas for meta-analysis, taxonomy of harms, and strategies for consistent use of information-gathering tools across services and over time, including setting and periodically reviewing standards for the relevant metrics and data.».

197. V. considerando 41, 45, 46, 53, 55, 56. artt. 13, 16, 18, 19 dell'EMFA. Per ulteriori riflessioni, v. anche quanto evidenzia HUSOVEC 2024, «The DSA's design has an implicit division of powers: parliaments make content rules and digital regulators only give the effect to them. This is why national and EU law are the sources of illegality, and why some of the DSA provisions explicitly only apply to illegal content (e.g. Article 16). The idea that the Commission could simply make on-the-go new content rules that would be specifically applicable to very large digital services has no support in the text of the Regulation. This division of powers has not only consequences for the separation of the executive from the legislative authority but also for the vertical division of powers between the Union and its Member States. If the European Commission were allowed to ad hoc regulate the illegality of content, it would encroach on the competencies that the Member States did not ask to be delegated through the Regulation. Thus, the attempt by the Commission to become a surrogate legislature would lead to an excess of its powers in two ways: an overreach of the executive, and an abuse of competence» (p. 52).

198. Text adopted by the Assembly on 1 October 2024 (26th sitting), cit.

199. Art. 45 del DSA.

Riferimenti bibliografici

- AA.VV. (2023), *Il Digital Services Act*, in L. Bolognini, E. Pelino, M. Scialdone (a cura di), "Digital Services Act e Digital Markets Act. Definizioni e prime applicazioni dei nuovi regolamenti europei", Giuffrè, 2023
- ASSOCIATION OF EUROPEAN RADIO (AER) (2022), *The Digital Services Act must safeguard freedom of expression online*, 18 January, 2022
- J. BARATA (2021), *The Digital Services Act and Its Impact on the Right to Freedom of Expression: Special Focus on Risk Mitigation Obligations*, Dsa Observatory, July 27, 2021
- M. BASSINI, O. POLLICINO (2023), *The reshaping of the freedom of expression in the digital environment in light of the role of social networks*, in A. Savin, J. Trzaskowski (eds.), "Research handbook on EU internet law", Edward Elgar Publishing, 2023
- L. BERTUZZI (2021), *Media exemption ruled out in DSA negotiations, but could return*, euractiv.com, 24 November 2021
- L. BOLOGNINI, E. PELINO, M. SCIALDONE (a cura di) (2023), *Digital Services Act e Digital Markets Act. Definizioni e prime applicazioni dei nuovi regolamenti europei*, Giuffrè, 2023
- S. BROUGHTON MICOVA, D. SCHNURR, A. CALEF, B. ENSTONE (2024) *Cross-Cutting Issues for DSA Systemic Risk Management: An Agenda for Cooperation*, Centre on Regulation in Europe (CERRE), 2024
- D. BUIJS (2021), *The Digital Services Act and the implications for news media and journalistic content (Part 1)*, Dsa Observatory, 2021
- I. BURI, J. VAN HOBOKEN (2022), *The Digital Services Act (DSA) proposal: a critical overview*, University of Amsterdam, 28 October 2022
- G. CAGGIANO (2021), *La proposta di Digital Service Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, aisdue.eu, 18 febbraio 2021, n. 1
- M. CANTERO GAMITO (2022), *Consistent regulatory and self-regulatory mechanisms for media freedom in the Digital Single Market. The European Media Freedom Act (EMFA) as meta-regulation*, RSCAS Working Papers 2022/42, European University Institute, 2022
- E. CAVASINO (2020), *Diritti e principi nello spazio giuridico europeo dei diritti fondamentali: un aspetto dell'esperienza costituzionale*, in "Rivista AIC", 2020, n. 1
- G. CERRINA FERONI (2024), *Informazione, un cambio di paradigma? L'impatto del Digital Services Act sul mondo dell'informazione*, Osservatorio sul giornalismo digitale, Report 2024
- P. CESARINI, G. DE GREGORIO, O. POLLICINO (2023), *The Media privilege in the European Media Freedom Act*, in "MediaLaws. Law and Policy of the Media in a Comparative Perspective", September 4, 2023
- M.L. CHIARELLA (2023), *Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment*, in "Athens Journal of Law", vol. 9, 2023, n. 1
- F. CHIRICO (2023), *La nuova frontiera della regolazione europea dei media e delle piattaforme: dal DSA all'EMFA*, in C. Contessa, P. Del Vecchio (a cura di), "Testo Unico Servizi Media e Audiovisivi. Annotato con dottrina e giurisprudenza D.lgs. 8 novembre 2021 n. 208", Editoriale Scientifica, 2023
- P. CHURCH (2023), *The Digital Services Act (DSA): A New Era for Online Harms and Intermediary Liability*, in "Global Privacy Law Review", vol. 4, 2023, n. 1
- L. CILIBERTI (2024), *Il nuovo regolamento AGCOM sui titoli abilitativi per la diffusione dei servizi di media audiovisivi – Tra promozione del mercato e oneri burocratici*, in "MediaLaws", 2024, n. 1

- L. CILIBERTI (2023), *Le ADR delle Autorità indipendenti. Tra tutela effettiva dei consumatori e deflazione del contenzioso giudiziale*, Wolters Kluwer Italia-CEDAM, 2023
- L. CILIBERTI (2022), *Free flow of information – Il contrasto alla disinformazione in tempi di guerra*, in “MediaLaws”, 2022, n. 2
- L. CILIBERTI, L. SANFILIPPO (2024), *La coregolamentazione e l'autoregolamentazione nella nuova Direttiva SMA*, in R. Mastroianni, O. Pollicino, M. Bassini (a cura di), “Il T.U. dei servizi di media audiovisivi”, Giuffrè, 2024
- Y.M. CITINO (2022), *Verso l'European Media Freedom Act: la strategia europea contro le minacce al pluralismo e all'indipendenza dei media da una prospettiva de iure condendo*, in “MediaLaws”, 2022, n. 2
- M. COLANTONI (2023), *I “servizi di piattaforma per la condivisione di video” nel TUSMA e i compiti di AGCOM*, in G. Cassano, C.E. Cazzato, F. Di Ciommo (a cura di), “Trattato delle garanzie nelle comunicazioni”, Giuffrè, 2023
- M.D. COLE, C. ETTELDORF, C. ULLRICH (2021), *Updating the Rules for Online Content Dissemination. Legislative Options of the European Union and the Digital Services Act Proposal*, Nomos, 2021
- G.L. CONTI (2018), *Manifestazione di pensiero attraverso la rete e trasformazione della libertà di espressione: c'è ancora da ballare per strada?*, Rivista AIC, 2018, n. 4
- M. CUNIBERTI (2022), *La professione del giornalista*, in G.E. Vigevari, O. Pollicino, C. Melzi d'Eril et al. (a cura di), “Diritto dell'Informazione e dei Media”, Giappichelli, 2022
- M. CUNIBERTI (2017), *Il contrasto alla disinformazione in rete tra logiche del mercato e (vecchie e nuove) velleità di controllo*, in “MediaLaws”, 2017, n. 1
- L. DANIELE (2020), *Diritto dell'Unione europea. Sistema Istituzionale – Ordinamento – Tutela giurisdizionale – Competenze*, con la collaborazione di S. Amadeo, G. Biagioni, C. Schepisi, F. Spitaleri, VIII ed., Giuffrè, 2020
- G. DE GREGORIO (2019), *From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society*, in “European Journal of Legal Studies”, vol. 11, 2019, n. 2
- F. DE STEFANI (2023), *Definizione e disciplina di: “destinatario”, “hosting”, “piattaforma” e “motori di ricerca”*, in L. BOLOGNINI, E. PELINO, M. SCIALDONE (a cura di), *Digital Services Act e Digital Markets Act. Definizioni e prime applicazioni dei nuovi regolamenti europei*, Giuffrè, 2023
- M. DEL MORAL SÁNCHEZ (2024), *The Devil is in the Procedure: Private Enforcement in the DMA and the DSA*, in “University of Bologna Law Review”, vol. 9, 2024, n. 1
- D. DERGACHEVA, V. KUZNETSOVA, R. SCHARLACH, C. KATZENBACH (2023), *One Day in Content Moderation. Analyzing 24 h of Social Media Platforms' Content Decisions through the DSA Transparency Database*, Center for Media, Communication, and Information Research (ZeMKI), Lab Platform Governance, Media, and Technology (PGMT), University of Bremen, 2023
- F. DONATI (2019), *La tutela dei minori nella Direttiva (UE) 2018/1808*, in G. Abbamonte, E. Apa, O. Pollicino (a cura di), “La riforma del mercato audiovisivo europeo”, Giappichelli, 2019
- N. EDER (2024), *Making Systemic Risk Assessments Work: How the DSA Creates a Virtuous Loop to Address the Societal Harms of Content Moderation*, in “German Law Journal”, 2024, forthcoming
- Z. EFRONI (2021), *The Digital Services Act: Risk-Based Regulation of Online Platforms*, in “Internet Policy Review”, November 2021
- EU DISINFO LAB (2023), *Policy Statement on Article 17 of the proposed European Media Freedom Act*, disinfo.eu, 24 January 2023

- EUROPEAN PUBLISHERS COUNCIL (2022), *European Commission unveils bold and ambitious Media Freedom Act*, 16 September 2022
- F. FERRARO (2019), *Vecchi e nuovi problemi in tema di efficacia diretta orizzontale della Carta*, in “federalismi.it”, 2019, n. 10
- L. FLORE (2023), *Disciplina dell’editoria e ordine dei giornalisti*, in G. Avanzini, G. Matucci, L. Musselli (a cura di), “Informazione e media nell’era digitale”, Giuffrè, 2023
- W. FOLKERT, S.L. KALÈDA, P.-J. LOEWENTHAL (2024), *The EU Digital Services Act*, online ed., Oxford University Press, 2024
- G. FROSIO, C. GEIGER (2023), *Taking fundamental rights seriously in the Digital Services Act’s platform liability regime*, in “European Law Journal”, November 2023
- C. GOANTA, T. BERTAGLIA, A. IAMNITCHI (2022), *The Case for a Legal Compliance API for the Enforcement of the EU’s Digital Services Act on Social Media Platforms*, in “FAccT ’22: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency”, Association for Computing Machinery, 2022
- G. GOSZTONYI, E. GALEWSKA, A. ŠKOLKAY (2024), *Challenges of Monitoring Obligations in the European Union’s Digital Services Act*, in “ELTE Law Journal”, 2024, n. 1
- O. GRANDINETTI (2022), *Il Testo unico per la fornitura dei servizi di media audiovisivi*, in “Giornale di diritto amministrativo”, 2022, n. 4
- O. GRANDINETTI (2022-A), *Le piattaforme digitali come “poteri privati” e la censura online*, in “Rivista italiana di informatica e diritto”, 2022, n. 1
- O. GRANDINETTI (2022-B), *Le piattaforme digitali tra libertà di impresa e libertà di espressione e di informazione*, in R. Mastroianni, F. Ferraro (a cura di), “Libertà di informazione e diritto dell’Unione europea. Le nuove sfide a tutela della democrazia e del pluralismo”, Editoriale Scientifica, 2022
- O. GRANDINETTI (2021), *Facebook vs. CasaPound e Forza Nuova, ovvero la disattivazione di pagine social e le insidie della disciplina multilivello dei diritti fondamentali*, in “MediaLaws”, 2021, n. 1
- O. GRANDINETTI (2012), *Il Tar Lazio sull’accesso alla piattaforma Sky*, in “Giornale di diritto amministrativo”, 2012, n. 7
- M. HUSOVEC (2024), *The Digital Services Act’s red line: what the Commission can and cannot do about disinformation*, in “Journal of Media Law”, vol. 16, 2024, n. 1
- S. LATTANZI (2022), *La lotta alla disinformazione nei rapporti tra Unione e Stati terzi alla luce del conflitto russo-ucraino*, in R. Mastroianni, F. Ferraro (a cura di), “Libertà di informazione e diritto dell’Unione europea. Le nuove sfide a tutela della democrazia e del pluralismo”, Editoriale Scientifica, 2022
- J. LAUX, S. WACHTER, B. MITTELSTADT (2021), *Taming the few: Platform regulation, independent audits, and the risks of capture created by the DMA and DSA*, in “Computer Law & Security Review”, vol. 43, 2021
- G. LO TAURO (2016), *Verso una tutela integrata dei diritti fondamentali in Europa. Il sistema multilivello di protezione e i rapporti tra ordinamenti: alla ricerca della tutela più estesa*, in “Fogli di lavoro per il Diritto Internazionale”, 2016, n. 4
- A. MAFFEO (2022), *La sottile linea di confine tra libertà di informazione e propaganda di guerra: il caso RT France*, in R. Mastroianni, F. Ferraro (a cura di), “Libertà di informazione e diritto dell’Unione europea. Le nuove sfide a tutela della democrazia e del pluralismo”, Editoriale Scientifica, 2022
- C. MALAVENDA, C. MELZI D’ERIL, G.E. VIGEVANI (2012), *Le regole del giornalismo. Istruzioni per un mestiere pericoloso*, il Mulino, 2012

- A. MANTELERO (2022), *Fundamental rights impact assessments in the DSA*, in “Verfassungsblog”, 1 November 2022
- M. MARONI, E. BROGI (2021), *Freedom of expression and the rule of law: the debate in the context of online platform regulation*, in P.L. Parcu, E. Brogi (eds.), “Research Handbook on EU Media Law and Policy”, Edward Elgar, 2021
- S. MARTINELLI (2023), *I contratti della Platform Economy. Ruoli e responsabilità delle piattaforme*, Giappichelli, 2023
- C. MASSA (2024), *L’European Media Freedom Act e il suo impatto sul Testo unico per la fornitura di servizi di media audiovisivi*, in R. Mastroianni, O. Pollicino, M. Bassini (a cura di), “Il T.U. dei servizi di media audiovisivi”, Giuffrè, 2024
- J. MCHANGAMA, N. ALKIVIADOU, R. MENDIRATTA (2022), *Thoughts On The Dsa: Challenges, Ideas and the Way Forward through International Human Rights Law*, The future of free speech, 2022
- I. McMILLAN (2019), *Enforcement Through the Network: The Network Enforcement Act and Article 10 of the European Convention on Human Rights*, in “Chicago Journal of International Law”, vol. 20, 2019, n. 1
- M. MONTI (2020), *La disinformazione online, la crisi del rapporto pubblico-esperti e il rischio della privatizzazione della censura nelle azioni dell’Unione Europea (Code of practice on disinformation)*, in “federalismi.it”, 2020, n. 11
- M. MONTI (2019), *Privatizzazione della censura e Internet Platforms: la libertà d’espressione e i nuovi censori dell’agorà digitale*, in “Rivista italiana di informatica e diritto”, 2019, n. 1
- L. MUSSELLI (2024), *La tutela dei minori tra media audiovisivi e servizi di condivisione video*, in R. Mastroianni, O. Pollicino, M. Bassini (a cura di), “Il T.U. dei servizi di media audiovisivi”, Giuffrè, 2024
- G. MUTO (2022), *European Media Freedom Act: la tutela europea della libertà dei media*, in “MediaLaws”, 2022, n. 3
- B. NASCIMBENE (2021), *Carta dei diritti fondamentali, applicabilità e rapporti fra giudici: la necessità di una tutela integrata*, European Papers, vol. 6, 2021, n. 1
- I. NENADIC, E. BROGI (2024), *The Game of Boards: The role of authorities in concerting the Digital Services Act and the Media Freedom Act for protecting media freedom*, in “MediaLaws. Law and Policy of the Media in a Comparative Perspective”, 28 August 2024
- S. NIKOLTCHEV (ed.) (2008), *IRIS Special: Editorial Responsibility*, European Audiovisual Observatory, 2008
- R. NIRO (2021), *Piattaforme digitali e libertà di espressione fra autoregolamentazione e coregolamentazione: Note ricostruttive*, in “Osservatorio sulle fonti”, 2021, n. 3
- K. PACUŁA (2024), *Inquiry into the validity of the Digital Services Act and the role of the representative associations under that regulation. Comments on the first decisions of the EU courts casting light on the DSA*, ERA Forum, vol. 25, 2024
- A. PALUMBO, J. PIEMONTE (2023), *Delega di funzioni regolamentari e lotta ai rischi sistemici causati dalla disinformazione nel Digital Services Act: quali rischi per la libertà di espressione?*, in “MediaLaws”, 2023, n. 3
- C. PAPAÉVANGELOU (2023), *‘The non-interference principle’: Debating online platforms’ treatment of editorial content in the European Union’s Digital Services Act*, in “European Journal of Communication”, vol. 38, 2023, n. 5
- P.L. PARCU, E. BROGI (eds.) (2021), *Research Handbook on EU Media Law and Policy*, Edward Elgar, 2021
- O. POLLICINO (2022), *Migrazioni di idee costituzionali e implicazioni per le opzioni rilevanti di politica del diritto: il caso della strategia europea contro la disinformazione on line*, in R. Mastroianni, F. Ferraro (a

- cura di), "Libertà di informazione e diritto dell'Unione europea. Le nuove sfide a tutela della democrazia e del pluralismo", Editoriale Scientifica, 2022
- O. POLLICINO (2019), *L'“autunno caldo” della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in "federalismi.it", 2019, n. 19
- O. POLLICINO (2018), *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*, in "MediaLaws", 2018, n. 3
- O. POLLICINO, G. DE GREGORIO (2024), *Le piattaforme di condivisione di video dalla Direttiva E-Commerce al Digital Services Act*, in R. Mastroianni, O. Pollicino, M. Bassini (a cura di), "Il T.U. dei servizi di media audiovisivi", Giuffrè, 2024
- O. POLLICINO, P. DUNN (2024), *Disinformazione e intelligenza artificiale nell'anno delle global elections: rischi (ed opportunità)*, in "federalismi.it", 2024, n. 12
- O. POLLICINO, P. DUNN (2024-A), *Intelligenza artificiale e democrazia, Opportunità e rischi di disinformazione e discriminazione*, Bocconi University Press, 2024
- E. PSYCHOGIOPOULOU (2022), *Judicial Dialogue and Digitalization: CJEU Engagement with ECtHR Case Law and Fundamental Rights Standards in the EU*, in "Journal of Intellectual Property, Information Technology, and Electronic Commerce Law", vol. 13, 2022, n. 2
- J.P. QUINTAIS, N. APPELMAN, R.Ó. FATHAIGH (2023), *Using Terms and Conditions to apply Fundamental Rights to Content Moderation*, in "German Law Journal", vol. 24, 2023, n. 5
- T. RODRÍGUEZ DE LAS HERAS BALLELL (2021), *The background of the Digital Services Act: looking towards a platform economy*, ERA Forum, vol. 22, 2021
- G. SCHLAG (2023), *European Union's Regulating of Social Media: A Discourse Analysis of the Digital Services Act*, in "Politics and Governance", vol. 11, 2023, n. 3
- V. SZÉP, R. WESSEL (2023), *Balancing restrictive measures and media freedom: RT France v. Council*, in "Common Market Law Review", vol. 60, 2023, n. 5
- D. TAMBINI (2021), *What is journalism? The paradox of media privilege*, in "European Human Rights Law Review", 2021, n. 5
- S. TOMMASI (2023), *The Risk of Discrimination in the Digital Market. From the Digital Services Act to the Future*, Springer, 2023
- I. TOURKOCHORITI (2023), *The Digital Services Act and the EU as the Global Regulator of the Internet*, in "Chicago Journal of International Law", vol. 24, 2023, n. 1
- Y. TSFATI, H.G. BOOMGAARDEN, J. STRÖMBÄCK et al. (2020), *Causes and consequences of mainstream media dissemination of fake news: literature review and synthesis*, in "Annals of the International Communication Association", vol. 44, 2020, n. 2
- J. VAN HOBOKEN, J.P. QUINTAIS, N. APPELMAN et al. (2023), *Putting the Digital Services Act Into Practice: Enforcement, Access to Justice, and Global Implications*, Amsterdam Law School Legal Studies Research Paper No. 2023-132023, 2023
- J.A. WINTER (1972), *Direct Applicability and Direct Effect Two Distinct and Different Concepts in Community Law*, in "Common Market Law Review", vol. 9, 1972, n. 4



DANIELLE BORGES

Media ownership transparency and the European Media Freedom Act: how did the EU get there?

The European Media Freedom Act (EMFA) brought a significant improvement to the disclosure of ownership information in the media sector, providing a clear framework on the types of information that media service providers should make available to the recipients of services. Given this context, this article aims at discussing the contribution that the EMFA rules on ownership transparency brings to the media environment, particularly with regards to improving media pluralism. In order to do that, the article explores the development and evolution of media ownership transparency as a concept in EU media law and policy. Then it discusses the implementation of the new rules and the challenges that it may pose to governments and the society at large.

EMFA – Media ownership – Transparency – Media pluralism

La trasparenza della proprietà dei media e il Regolamento europeo sulla libertà dei media: come ci è arrivata l'UE?

Il Regolamento europeo sulla libertà dei media (EMFA) ha apportato un miglioramento significativo riguardo la trasparenza delle informazioni sulla proprietà nel settore dei media, dettando un quadro chiaro sul tipo di informazioni che i servizi di media devono fornire alle autorità e al pubblico in generale. Alla luce di questo nuovo quadro normativo, questo articolo si propone di analizzare il contributo che le regole a tutela della trasparenza previste nell'EMFA possono apportare al settore dei media, in particolare per quanto riguarda il miglioramento del pluralismo. A tal fine, l'articolo esamina lo sviluppo e l'evoluzione della trasparenza della proprietà dei media come concetto nella legislazione e nella politica dell'Ue, nonché le sfide nell'attuazione delle nuove regole sulla trasparenza previste nell'EMFA.

EMFA – Proprietà nel settore dei media – Trasparenza – Pluralismo dei media

The Author is Research Associate at the Center for Media Pluralism and Media Freedom - Robert Schuman Centre, European University Institute

This paper is part of the monographic section *EMFA under the spotlight: towards a common regulatory framework to foster media pluralism?* edited by Elda Brogi

SUMMARY: 1. Introduction. – 2. Brief historical overview of the media transparency debate at EU level: from Council of Europe resolutions to EMFA. – 3. Transparency obligations in EMFA: Article 6. – 4. Challenges ahead. – 5. Conclusions.

1. Introduction

Transparency is a complex and multidimensional concept that can be applied to the different sectors of society and in different stages of governance or decision-making processes, from the launch of an action or project to its outcomes¹.

Different from other private sectors in which transparency has been consolidated as an important concept and principle for years, such as banking and finance, in the media sector transparency has evolved gradually, and only in recent years it emerged as a relevant principle and requirement applied to media policy and regulation², gaining however an enormous relevance, due to its contribution to quality journalism and, as a consequence, to democracy.

Though transparency can also be considered a general guiding principle, its multidimensional aspect allows us to distinguish in a more specific way the different dimensions or segments of a certain business or service to which transparency can be applied. In the media sector, it is possible to identify at least three different dimensions of the application of transparency. First, transparency of ownership relates to the structure of the medium itself and aims to make visible information on the owners of media outlets, including beneficial owners. Second, transparency can be applied to the financial aspect of a media business, requiring them to disclose information on revenues, including resources re-

ceived from private donors or public funds. Third, transparency can be applied to editorial decisions, requiring newsrooms to disclose conflicts of interest that might influence content.

This article will focus on the dimension or aspect of transparency that concerns ownership. Media ownership transparency pursues several specific goals, such as, avoiding the concentration of media markets, protecting quality journalism, reinforcing audience credibility, avoiding political influence over content and conflicts of interest. Altogether, these specific goals contribute to media pluralism and diversity. But most and above all media ownership transparency contributes to “forming well-informed opinions and, consequently, for actively participating in a democracy” (Recital 32, Regulation (EU) 2024/1083). It is no coincidence that the “European Democracy Action Plan”³ proposes the strengthening of independent media as one of the three pillars to make democracy more resilient in the bloc. And one of the measures foreseen in the document is the development of a media ownership monitor. This shows that transparency and democracy are inseparable concepts. Therefore, ownership transparency becomes of crucial importance in times of important threats to democracy happening not only in Europe but all around the world.

Another facet of the multidimensional character of transparency relates to the beneficiaries or re-

1. BORGES-CHRISTOPHOROU 2024.

2. FIGUEIRA-COSTA E SILVA 2023.

3. European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions On the European democracy action plan, [COM\(2020\) 790](#).

cipients of the information disclosed. In the media sector, it is possible to identify two different dimensions. One refers to the civic dimension – also named by some authors as downwards transparency⁴ – according to which the information disclosed is scrutinized by the civil society, investors and the general public. The other is called the administrative dimension – or upwards transparency⁵ – and relates to the disclosure of information to regulatory bodies and the government in general⁶.

Given the prominence that media ownership transparency has assumed in recent years and its role in supporting democracy, this article aims to explain how the European Media Freedom Act – EMFA (Regulation (EU) 2024/1083) can enhance transparency of media ownership in the European Union. The article is structured in three parts; the first one provides a historical overview of the development and evolution of the idea of ownership transparency in EU media policy. The second part analyzes the contribution that the EMFA brings to the media environment, whereas the third part concentrates on the challenges that the implementation of media ownership transparency rules poses to governments and the society at large.

2. Brief historical overview of the media transparency debate at EU level: from Council of Europe resolutions to EMFA

The debate over ownership transparency in EU media policy is a corollary of the debate on pluralism. Indeed, the initial discussions over media own-

ership transparency were restricted to ownership structure and the avoidance of monopolies⁷. At the European level, still in the 1970's, the Committee of Ministers of the Council of Europe has adopted Resolution 74(43) on press concentrations⁸. At the EU level, the issue of concentration gained greater relevance in the mid-80's in the aftermath of the decline of state monopoly broadcasting but the first specific acknowledgement of "pluralism" came with the publication of the 1992 Green Paper on "Pluralism and Media Concentration in the Internal Market: An Assessment of the Need for Community Action" by the European Commission⁹. From the 1990's the debate on media transparency gained its own visibility; the Council of Europe issued Recommendation 94(13) on media transparency¹⁰ and Recommendation 99(1) on pluralism¹¹. These were subsequently updated with the adoption of new documents aiming at responding to emerging challenges, culminating with Recommendation CM/Rec (2018)1[1] on media pluralism and transparency on media concentrations¹². This document explicitly recognises the role played by ownership transparency – with the disclosure of ownership structures behind the media – in promoting media pluralism and democracy in general. Furthermore, Recommendation CM/Rec (2018)1[1] is a comprehensive document, including an appendix with guidelines that set out requirements and institutional frameworks for ensuring media pluralism. Within the institutional framework, the document lists supporting measures that can help states

4. CRAUFURD SMITH–KLIMKIEWICZ–OSTLING 2021.

5. *Ibidem*.

6. FIGUEIRA–COSTA E SILVA 2023.

7. TOMAZ 2024.

8. Council of Europe, Resolution 74(43) on press concentrations. Adopted by the Committee of Ministers on December 16, 1974, at the 240th meeting of the Ministers' Deputies.

9. EUROPEAN COMMISSION 1992.

10. Council of Europe, Recommendation No. R (94) 13 of the Committee of Ministers to member states on measures to promote media transparency. Adopted by the Committee of Ministers on November 22, 1994, at the 521st meeting of the Ministers' Deputies.

11. Council of Europe, Recommendation No. R (99) 1 of the Committee of Ministers to member states on measures to promote media pluralism. Adopted by the Committee of Ministers on January 19, 1999, at the 656th meeting of the Ministers' Deputies.

12. Council of Europe, Recommendation CM/Rec (2018)1[1] of the Committee of Ministers to member States on media pluralism and transparency of media ownership. Adopted by the Committee of Ministers on 7 March 2018 at the 1309th meeting of the Ministers' Deputies.

achieve pluralism, including ownership control and transparency requirements, and is very specific about the information that media providers should make available to the public and authorities. In this regard, point 4.5 of Recommendation CM/Rec (2018)1[1] mentions: (i.) legal name and contact details of a media outlet; (ii.) name(s) and contact details of the direct owner(s) with shareholdings enabling them to exercise influence on the operation and strategic decision making of the media outlet. States are recommended to apply a threshold of 5% shareholding for the purpose of disclosure obligations; (iii.) name(s) and contact details of natural persons with beneficial shareholdings. Beneficial shareholding applies to natural persons who ultimately own or control shares in a media outlet or on whose behalf those shares are held, enabling them to indirectly exercise control or influence on the operation and strategic decision making of the media outlet; (iv.) information on the nature and extent of the shareholdings or voting rights of the above legal and/or natural persons in other media, media-related or advertising companies which could lead to decision-making influence over those companies, or positions they may hold in political parties; (v.) name(s) of the persons with actual editorial responsibility; and (vi.) changes in ownership and control arrangements of a media outlet.

In addition, point 4.7 of Recommendation CM/Rec (2018)1[1] encourages Member States to adopt measures to ensure high levels of transparency with regards to the sources of financing of media outlets obtained through State funding mechanisms, such as advertising, grants and loans, as well as the disclosure of information on “contractual relations with other media or advertising companies and political parties that may have an influence on editorial independence”¹³. Furthermore, according to the Recommendation, a national authority or designated body should be entrusted with the role of storing and making ownership information accessible to the public free of charge, without delay, and, for instance, in the format of online databases, in open formats (point 4.8).

At the EU level, the first specific recognition in a legal document of the need for and the role of media ownership transparency in democratic media systems appears in the 2018 amendment of the Audiovisual Media Services Directive (AVMSD). In this context, recitals 15 and 16 justify the need for disclosure of ownership information, but the previous wording of Article 5 is maintained, thus leaving it to the discretion of Member States to require information on beneficial ownership from media service providers (Article 5(2)).

At the same time, the EU invested in research on media ownership, which made possible the collection and availability of comprehensive information in the form of databases containing information on ownership and control of the most relevant news media in all EU Member States, as well as media ownership laws and relations between digital platforms and news media. This is the case, for instance, of the Euromedia Ownership Monitor (EurOMo)¹⁴ and of the Media Ownership Monitor¹⁵.

Then, in 2022, building up on the guidelines proposed by the Recommendation, the EU included transparency obligations among the obligations of media service providers under the proposal for a European Media Freedom Act Proposal (EMFA), whose final text was adopted in April 2024, containing specific rules on media ownership transparency obligations. Having this in mind, the article turns now to the analysis of the ownership disclosure requirements required by Article 6 EMFA.

3. Transparency obligations in EMFA: Article 6

Article 6 is extremely important to the proper provision of media services and to the good functioning of the media market. By imposing different transparency obligations on media providers, EMFA demonstrates its commitment to the principle of transparency in its different aspects. Transparency is not only a fundamental principle but also a requirement in democratic societies; it enables

13. Council of Europe, Recommendation CM/Rec (2018)1[1] of the Committee of Ministers to member States on media pluralism and transparency of media ownership. Adopted by the Committee of Ministers on 7 March 2018 at the 1309th meeting of the Ministers’ Deputies.

14. [Euromedia Ownership Monitor \(EurOMo\)](#).

15. [Media Ownership Monitor](#).

individuals to make informed decisions about the exercise of power and hold governments accountable for their exercise of power¹⁶. The transparency obligations provided by Article 6 EMFA are further promoted by Commission Recommendation (EU) 2022/1634 of 16 September 2022 on internal safeguards for editorial independence and ownership transparency in the media sector.

The obligations contained in Article 6, under the Title of Duties of Media Service Providers, aim at different objectives and to the disclosure of different types of information. While Article 6(1) and (2) are concerned with the disclosure of ownership and financial information of media service providers, Article 6(3) concerns measures to guarantee editorial independence, including the disclosure of conflicts of interest by media services providers. This paper, however, concentrates on the obligations related to media ownership and thus on Article 6(1) and (2).

Recitals 32 and 33 EMFA explain the motivation behind the disclosure of ownership information and structure to the recipients of media service providers. The recitals refer to the economic and non-economic aspects of transparency: on the one hand, the disclosure of ownership and financial information of media providers allows users of services to know who owns and is behind a media outlet media, thus enabling them to identify potential conflicts of interest; on the other hand the availability of information on media ownership, its structures and financial aspects contributes to a fair and healthy media market environment, enhances accountability and control, as it allows governments and national authorities to verify compliance with competition rules, contributing to the quality of media services and to the EU internal market as a whole. Moreover, this motivation also demonstrates that EMFA encompasses both the civic and administrative dimensions of transparency, also called downwards and upwards transparency¹⁷.

Therefore, the wording of these Recitals shows that the objective of ensuring ownership transparency in the media market is not restricted only to

the economic, corporate or criminal aspect, as is the case of commercial and anti-money laundering laws, such as Directive 2015/849. As claimed by Craufurd-Smith, Klimkiewicz and Ostling¹⁸, corporate transparency requirements are not specifically tailored to address media-related concerns. Therefore, Article 6 has a strong commitment with protecting editorial independence and the readership/audience, reinforcing the right of citizens to choose their source of information freely and consciously and allowing also other actors, such as journalists, watchdogs and researchers, to independently monitor possible misconduct, conflicts of interest and abuse of power in the media sector.

With these aims expressed by legislators, Article 6(1) EMFA requires media service providers to make the following information easily and directly accessible to the recipients of their services: (a) their legal name or names and contact details; (b) the name or names of their direct or indirect owner or owners with shareholdings enabling them to exercise influence on the operation and strategic decision making, including direct or indirect ownership by a state or by a public authority or entity; (c) the name or names of their beneficial owner or owners as defined in Article 3, point (6), of Directive (EU) 2015/849; (d) the total annual amount of public funds for state advertising allocated to them and the total annual amount of advertising revenues received from third-country public authorities or entities.

The information required under Article 6(1) is quite similar to that mentioned under point 4.5 and 4.7 of Recommendation CM/Rec (2018)1[1]. In effect, even before the EMFA adoption, some Member States had already put in place legislative frameworks that required media service providers to disclose such information. Some countries, for instance, improved their media ownership transparency requirements by adopting/changing their laws to comply with the Anti-Money Laundering Directive. However, in the absence of a harmonised media specific framework, the situation remained fragmented across the EU in terms of the disclosure of media ownership information as

16. BORGES-CHRISTOPHOROU 2024.

17. CRAUFURD SMITH-KLIMKIEWICZ-OSTLING 2021.

18. *Ibidem*.

demonstrated by the Media Plurality and Diversity Online Study¹⁹. Another problem pointed out by the study is the different levels of disclosure in different Member States, with problems such as missing information; outdated information; information not made available to the general public; or information not presented in friendly format files.

In this regard, Article 6(2) can be considered an important measure to tackle the differences in the disclosure of ownership information found across the EU. It builds up on point 4.8 of Recommendation CM/Rec (2018)1[1] and on Section III of Recommendation (EU) 2022/1634. EMFA does not specify which authority is responsible for storing this information, stating that “Member States shall entrust national regulatory authorities or bodies or other competent authorities or bodies with the development of national media ownership databases containing the information set out in paragraph 1.” Therefore, Member States have the possibility to use other databases already existing in their legal framework, such as the one under Article 30 of the Anti-Money Laundering Directive (Directive 2015/849/EU) or commercial registers databases, adding and adapting the specific information required under Article 6(1) points (a) to (d).

Therefore, as this section shows, by requiring media service providers to provide their users with easy and direct access to ownership information, including beneficial owners, EMFA strengthens the right of citizens to freely and consciously choose their source of information, to be aware of the potential inclination or bias (political or economic) of a media service in light of its ownership, and to enable journalists, researchers, and national authorities to monitor possible misconduct or abuse of power in the media sector.

Nevertheless, the full implementation of the transparency obligations analysed in this section across the EU may not be an easy task and will require a major coordination effort by the European Commission, the European Board for Media Services, and national authorities and governments. In the next section, therefore, the article attempts to discuss the challenges ahead in terms of the implementation of the EMFA ownership transparency rules.

4. Challenges ahead

One of the challenges for the full enforcement of this new provision in EMFA is the argument raised in the recent decision of the Court of Justice of the European Union (CJEU) on Joined Cases C-37/20 and C-601/20 which declared invalid point (c) of the first subparagraph of Article 30(5) of the Anti-Money Laundering Directive requiring Member States to ensure that information on beneficial ownership is accessible to the general public in all cases. However, it is important to note that granting the general public access to information on beneficial ownership can potentially interfere with fundamental rights, such as the protection of personal data and the respect for private life. Although ownership transparency in EMFA has a broader scope than combating money laundering and journalists are not affected by the mentioned CJEU decision, there is a possible risk for the future enforcement of EMFA's Article 6 when it comes to the disclosure of media ownership to the general public.

In order to avoid this fundamental rights' conflict, Recital 32 EMFA explains that, in the context of media systems, “the disclosure of targeted media ownership information would produce benefits clearly outweighing any possible impact of the disclosure obligation on fundamental rights, including the right to private and family life and the right to protection of personal data. In that context, the measures taken by Member States under Article 30(9) of Directive (EU) 2015/849 of the European Parliament and of the Council (11) should not be affected.”

Another challenge will be on how to standardise the provision of ownership information. Recital 32 provides some guidance, stating that “The required information should be disclosed by the relevant media service providers in an electronic format, for instance on their websites, or another medium that is easily and directly accessible.” This task may be easier at national level, but if the aim is for national authorities to build databases that allow for cross-country/cross-jurisdictional searches, this will require coordination efforts at EU level. In effect, considering that Article 6 EMFA will also affect the disclosure of ownership information in

19. EUROPEAN COMMISSION 2022.

the audiovisual sector and thus have an impact on the application of Article 5(2) AVMSD (Directive 2010/13/EU), Recital 46 EMFA recognises that the implementation of this provision of the AVMSD in conformity with Article 6 EMFA will require guidelines from the EC with the assistance of the European Board for Media Services, in order to achieve legal certainty in that field.

Finally, while acknowledging the progress made by the ownership rules provided by EMFA, it can be said that there is still important information that is not included in Article 6 (1). According to Tomaz²⁰, in terms of the financial information to be disclosed by media providers, EMFA has focused mainly on public funding (Article 6(1) (d)), but the absence of comprehensive systematic information on news media revenues, including private funding, may reveal an extremely partial and distorted picture in this respect.

5. Conclusions

Ownership transparency applied to the media sector started to be discussed during the 1970s. However, it was only in recent years that it gained shape and importance, pushed by academic studies on media pluralism and the Council of Europe work in the field. The evolution of the idea of media ownership transparency gradually made clear its relevance as a crucial element for the effective functioning of democracies. It contributes to pluralism in various ways by preventing abuses of media power, editorial influence, and media

concentration, besides strengthening trust and respect in journalism. Transparency also empowers citizens to fully exercise their right to freedom of expression and gain a more critical understanding of the information they receive. In turn, the heightened ability to evaluate information enables citizens to make informed choices, a necessary element in democratic societies²¹.

While EMFA represents a major advancement on the harmonisation of the disclosure of media ownership information, there are some challenges ahead on the implementation of the transparency rules. To begin with, there is the possibility of this provision being challenged before courts for alleged conflict with other fundamental rights, especially privacy and private life, under similar arguments as the one raised on Joined Cases C-37/20 and C-601/20. Secondly, major coordination efforts will be required from the Commission and the European Board for Media Services, in order to provide guidance and avoid legal uncertainty in the implementation of the rules at national level. Thirdly, there will likely still be some gaps regarding the information on news media revenues, as EMFA does not require the provision of information of private funding.

Transparency of ownership in the media sector is, after all, a piece of a larger puzzle of building media pluralism; it is certainly an important piece, but not the only one contributing to diversity, freedom of information, quality journalism and, as a consequence, to an informed citizenry.

References

- R. CRAUFURD SMITH, B. KLIMKIEWICZ, A. OSTLING (2021), *Media ownership transparency in Europe: Closing the gap between European aspiration and domestic reality*, in "European Journal of Communication", vol. 36, 2021, n. 6
- D. BORGES, C. CHRISTOPHOROU (2024), *Understanding the democratic role of media ownership transparency*, in E. Brogi, I. Nenadić, P.L. Parcu (eds.), "Media Pluralism in the Digital Era. Legal, Economic, Social, and Political Lessons Learnt from Europe", Routledge, 2024
- EUROPEAN COMMISSION (2022) - Directorate-General for communications networks, content and technology - P.L. Parcu, E. Brogi, S. Verza et al., *Study on media plurality and diversity online: final report*, Publications Office of the European Union, 2022

20. TOMAZ 2024.

21. BORGES-CHRISTOPHOROU 2024.

EUROPEAN COMMISSION (1992), *Pluralism and Media Concentration in the Internal Market – An Assessment of the Need for Community Action Commission Green Paper*, COM(92) 480, 23 December 1992

A. FIGUEIRA, E. COSTA E SILVA (2023), *Transparency as a quality dimension: media ownership and the challenges of (in)visibility*, in “Qualidade do Jornalismo”, 2023, n. 44

T. TOMAZ (2024), *Media ownership and control in Europe: A multidimensional approach*, in “European Journal of Communication”, vol. 39, 2024, n. 5

Sezione monografica

Digitalizzazione del processo e diritti fondamentali.
Profili processuali

a cura di

Francesca Bailo e Michele Francaviglia



**RIVISTA ITALIANA DI
INFORMATICA E DIRITTO**

PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0200 • articolo non sottoposto a peer review • pubblicato in anteprima il 20 dic. 2024
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale 

FRANCESCA BAILO – MICHELE FRANCAVIGLIA

Digitalizzazione del processo e diritti fondamentali – Profili processuali

Introduzione

F. Bailo è professoressa associata di Diritto costituzionale presso il Dipartimento di Giurisprudenza - Università degli studi di Genova

M. Francaviglia è ricercatore di Diritto costituzionale presso il Dipartimento di Giurisprudenza - Università degli studi di Genova

Questo contributo fa parte della sezione monografica *Digitalizzazione del processo e diritti fondamentali – Profili processuali* a cura di Francesca Bailo e Michele Francaviglia

La pressoché integrale digitalizzazione del processo, insieme al potenziamento delle risorse umane in ambito giudiziario (essenzialmente attraverso la messa in funzione degli Uffici per il processo), rappresentano i due cardini attorno a cui ruota l'ambizioso obiettivo della riduzione dei tempi del processo che, com'è noto, è un caposaldo della c.d. riforma Cartabia.

Il Seminario “*Process digitalization and fundamental rights*”, di cui oggi presentiamo gli atti, è stato incentrato sul primo dei due aspetti appena richiamati, avendo cura di traghettare il fenomeno della digitalizzazione in ambito giudiziario con un approccio interdisciplinare, non schiacciato su delle prospettive meramente settoriali e prive di una visione d'insieme. A tal fine, l'incontro di studio – tenutosi presso l'Università di Genova il 9 maggio 2024 e organizzato nell'ambito del progetto “*Law and regulation for a better-safe Cyberspace*” (CYBERRIGHTS - Partenariato esteso SERICS Spoke 1) in sinergia con il progetto PRIN PNRR 2022 su “*Digitalization of the judiciary functions: trends, perspectives and risks*” – si è avvalso del prezioso e corale contributo di numerosi esperti in materia costituzionale, privatistica, processualprivatistica e processualpenalistica, consentendo così di fare il punto su questo complesso percorso di ammodernamento del “servizio giustizia”.

Si è ritenuto opportuno raccogliere le relazioni e gli interventi di questa proficua giornata di studio, debitamente aggiornati e rielaborati, in due separate sezioni monografiche: una specificamente dedicata agli aspetti processualistici e, ancor prima, al rilievo costituzionale dell'accesso alla rete come risorsa indispensabile, oggi, tra l'altro, al diritto ad una tutela giurisdizionale effettiva; l'altra, che comparirà sul fascicolo 1/2025 di questa Rivista, maggiormente concentrata sull'analisi dei profili sostanziali, pubblicistici e privatistici, connessi all'impiego (in atto o potenziale) delle nuove tecnologie in detto specifico ambito.

Prima di entrare *in medias res*, e senza voler anticipare le relazioni che seguiranno, ci si limita a sottolineare come il nesso funzionale tra l'*efficienza/efficacia* dei servizi di giustizia e l'*effettività* di alcuni diritti fondamentali richieda di misurare come la digitalizzazione del primo incida sulla seconda, sia in termini di certezza del diritto, sia in termini di parità di accesso alla tutela giurisdizionale, sia, infine, in termini di sicurezza dei dati giudiziari e del loro trattamento. Ciò al precipuo fine di vagliare i vantaggi e le criticità legate all'utilizzo degli strumenti informatici e di intelligenza artificiale da parte sia degli operatori del diritto che dei cittadini e delle imprese.

Al riguardo, com'è noto, cominciano ad affiorare nel panorama normativo i primi tentativi di regolazione di quella che ben può definirsi come una nuova “frontiera del diritto”.

In tal senso, occorre senz'altro menzionare, quale “faro” che potrebbe illuminare il percorso verso un impiego consapevole e responsabile delle nuove tecnologie nell'ambito dei procedimenti giudiziari, la Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi”, approvata dalla Commissione europea per l'efficienza della giustizia (CEPEJ) nel dicembre 2018 e che, pur essendo uno strumento di *soft law*, mira ad assumere un ruolo centrale nella creazione di un quadro normativo e valoriale comune a livello europeo. A questa devono poi aggiungersi, sul versante eurounitario, il forse meno noto regolamento Ue 2023/2844 del 13 dicembre 2023 sulla digitalizzazione della cooperazione giudiziaria e dell'accesso alla giustizia in materia civile, commerciale e penale a livello transfrontaliero, applicabile dal 1° maggio 2025 e il più recente Regolamento sull'AI (c.d. *AI Act*). Sul fronte interno, occorre poi dar conto del fatto che il Consiglio dei ministri, il 23 aprile 2024 ha approvato, su proposta del Presidente Giorgia Meloni e del Ministro della giustizia Carlo Nordio, un disegno di legge (l'A.S. 1146) per l'introduzione di disposizioni e la delega al Governo in materia di intelligenza artificiale,

andando così a integrare – nelle intenzioni degli estensori – il quadro regolatorio rispetto a quegli spazi non raggiunti dall'*AI Act*.

Ebbene, l'approccio interdisciplinare adottato negli odierni contributi ha il pregio – tra gli altri – di mettere bene in evidenza gli elementi di criticità e le potenzialità degli assetti prospettati da siffatti plessi regolatori, commisurandoli peraltro agli stessi target utilizzati a livello internazionale e/o eurounitario per misurare l'efficienza del settore giustizia; non solo: ampia attenzione viene riservata sia alle implicazioni teorico-giuridiche che ben possono derivare dell'impiego in ambito giudiziario delle più recenti innovazioni tecnologiche a disposizione (quale può essere considerata l'intelligenza artificiale generativa), sia agli sviluppi e ai possibili scenari dinanzi ai quali dette innovazioni potrebbero porre il giurista in un futuro non troppo lontano.

Chiaramente, è bene precisarlo, si tratta di una linea di ricerca tutt'altro che in via di esaurimento, sicché le risposte che potranno rinvenirsi in questi lavori devono ancora ritenersi strutturalmente provvisorie; del resto, ci troviamo dinanzi ad una rivoluzione globale dell'universo digitale che, in relativamente poco tempo, ha stravolto le precedenti coordinate e che – verosimilmente – è destinato ad inaugurare una nuova stagione, dai tratti ancora incerti; un nuovo orizzonte che, come sempre accade in questi casi, alimenta sentimenti tra loro fortemente contrastanti: paure e pregiudizi, o, al contrario, entusiasmi smisurati.

Nei contributi che seguiranno, ferma la consapevolezza di non poter giungere a risposte definitive sul tema, si è senz'altro cercato di superare tale ultima dicotomia – tra "apocalittici e integrati", verrebbe da dire – e di fare i conti, nel modo più obbiettivo possibile, con la sfida che l'IA ha lanciato ad assetti e a costruzioni giuridiche consolidati da tempo, talora da secoli.



PAOLO COMOGLIO

AI Act e consulenza legale online: problemi in tema di accesso alla giustizia

Il saggio esamina l'impatto dell'intelligenza artificiale generativa sul modello tradizionale di avvocatura, evidenziando i rischi per il monopolio degli avvocati nella consulenza legale. L'uso dell'intelligenza artificiale nella consulenza potrebbe rendere incerti i confini tra attività legale vera e propria e attività commerciale, ponendo come sempre più attuale il problema dell'esercizio abusivo della professione e della necessità di una regolamentazione specifica. In particolare, nella prospettiva di questo saggio, l'AI Act non considera adeguatamente i rischi di strumenti di intelligenza artificiale nel contesto legale, mettendo potenzialmente a rischio l'accesso alla giustizia e la trasparenza delle decisioni algoritmiche.

Intelligenza artificiale – Accesso alla giustizia – Legal tech – AI Act – Esercizio abusivo professione legale

AI Act and online legal advice: issues regarding access to justice

The essay examines the impact of generative artificial intelligence on the traditional model of legal practice, highlighting the risks to the monopoly lawyers hold in legal consultancy. The use of AI in legal advice could blur the boundaries between genuine legal practice and commercial activities, raising the increasingly relevant issue of unauthorized practice of law and the need for specific regulation. In particular, from the perspective of this essay, the AI Act does not adequately address the risks posed by AI tools in the legal context, potentially jeopardizing access to justice and the transparency of algorithmic decision-making.

Artificial Intelligence – Access to justice – Legal tech – AI Act – Unauthorized practice of law

L'Autore è professore associato in Diritto processuale civile presso l'Università degli studi di Genova

Questo lavoro è stato parzialmente finanziato dal progetto NextGenerationEU “Security and Rights in CyberSpace” (SERICS) e dal progetto NextGenerationEU “Digitalization of the judiciary functions: trends, perspectives and risks” (PRIN PNRR, Codice progetto: P2022PRBCS, CUP D53D23022420001)

Questo contributo fa parte della sezione monografica *Digitalizzazione del processo e diritti fondamentali – Profili processuali* a cura di Francesca Bailo e Michele Francaviglia

SOMMARIO: 1. Il modello tradizionale di avvocatura. – 2. Tecnologie v. semplificazione del diritto: IA generativa ed esercizio non autorizzato della professione forense. – 3. Il tramonto del monopolio degli avvocati? – 4. *Legal tech* e AI Act: necessità di una regolamentazione *ad hoc* per la consulenza legale online?

1. Il modello tradizionale di avvocatura

L'idea moderna di avvocatura si basa su due pilastri, ovvero l'indipendenza e l'esclusività. E si può dire che è proprio a queste prerogative che si ricollega la tradizionale negazione della natura imprenditoriale della professione legale¹. Questo modello unitario è sostanzialmente diffuso in quasi tutti gli ordinamenti² e, tranne alcuni casi (come la Cina³), ha influenzato anche gli ordinamenti dove la disciplina dell'avvocatura è ancora piuttosto recente⁴.

Infatti, pur con notevoli differenze, è opinione diffusa che l'avvocato svolga una duplice funzione: assistere i propri clienti, ma anche collaborare al buon funzionamento della giustizia, consigliando correttamente i propri clienti ed evitando un uso distorto e abusivo degli strumenti di tutela

giudiziaria⁵. In altre parole, il compito dell'avvocato è quello di garantire una consulenza qualificata, competente e indipendente (sia dal cliente che da altri soggetti)⁶. Si afferma spesso, inoltre, che in molti casi l'avvocatura ha contribuito al mantenimento dello Stato di diritto⁷.

Questa duplice funzione è riconosciuta espressamente anche dai tribunali internazionali, come, ad esempio, dalla Corte europea dei diritti dell'uomo, nella decisione *Nikula c/Finlandia*⁸, e dalla Corte di giustizia dell'Unione europea, nella decisione *Prezes Urzędu Komunikacji Elektronicznej c/Commissione*⁹.

Proprio per questa duplice funzione, la regolamentazione della professione legale è diffusamente caratterizzata da tre prerogative: le barriere all'ingresso, gli statuti che regolano

1. HAZARD-DONDI 2001; DEFFAINS 2023.

2. HAZARD-DONDI 2004; REMUS 2014; DONDI-ANSANELLI-COMOGLIO 2017, p. 37; COMOGLIO 2022, p. 99.

3. ASAI 2011; XU 2022; WANG 2019.

4. KITAMURA 2023; MIYAGAWA-NASU-KOYAMA-KUBORI 1992; MIYATA 2021.

5. Su questa concezione profondamente radicata, si veda in generale HAZARD-DONDI 2004; HAZARD-DONDI 2006, nonché, con specifico riferimento ai sistemi di common law, LUBAN 1988, RHODE 2000.

6. DAVIS 2003, pp. 1281-1282, REMUS-LEVY 2017, p. 545.

7. REMUS 2017, pp. 807, 864-865 (che osserva che «Un quadro stabile del diritto, a sua volta, richiede avvocati indipendenti, impegnati nelle dinamiche relazionali di fiducia, lealtà, giudizio, responsabilizzazione e servizio»), CASERTA-MADSEN 2019, p. 14. In una prospettiva storica, si veda SÉVE 2023.

8. *Nikula contro Finlandia*, caso 31611/96, (Corte europea dei diritti dell'uomo), sentenza del 30 novembre 2000 [ECLI:CE:ECHR:2002:0321JUD003161196].

9. *Prezes Urzędu Komunikacji Elektronicznej/Commissione*, cause riunite C-422/11 P e C-423/11 P (CGUE), sentenza 6 settembre 2012 [ECLI:EU:C:2012:553].

l'esercizio non autorizzato della professione¹⁰ e i codici deontologici¹¹.

In realtà, a partire dai primi anni Ottanta, questo modello unitario si è segmentato, soprattutto negli Stati Uniti e nelle giurisdizioni con economie più forti¹². Si tratta di un fenomeno certamente noto (caratterizzato soprattutto dall'emergere di grandi studi legali) e, soprattutto nel contesto statunitense, definito *Big Law*¹³.

Pur differenziandosi, entrambi questi due modelli di avvocatura (avvocati tradizionali e grandi studi legali) si fondano sull'esclusività dell'attività di consulenza legale, partendo dal presupposto che esista un confine tra la pratica legale e la pratica commerciale¹⁴. Questo modello tradizionale è tuttavia rimasto immutato fino ad oggi, anche se la presenza di barriere all'accesso alla professione e le stesse regole di etica legale sono state messe seriamente in discussione¹⁵.

L'uso dell'intelligenza artificiale generativa può mettere in discussione queste prerogative tradizionali dell'avvocatura. Più specificamente, l'intelligenza artificiale può rompere il monopolio degli avvocati sulla consulenza legale in un duplice senso, da un lato rendendo il diritto direttamente accessibile a persone non preparate in legge e, dall'altro, aprendo il mercato della consulenza legale a non avvocati.

2. Tecnologie v. semplificazione del diritto: IA generativa ed esercizio non autorizzato della professione forense

In realtà, si può dire che ogni innovazione tecnologica abbia avuto un'influenza significativa sull'attività legale¹⁶. Si pensi, ad esempio, ai formulari.

Prima dell'invenzione della stampa (quando era certamente difficile e costoso redigere documenti scritti), i formulari erano utilizzati principalmente dalle burocrazie statali e dai notai. Dall'invenzione della stampa, il loro uso si è diffuso, rendendoli veri e propri ausili all'attività professionale¹⁷.

In ogni caso, fino ad oggi le innovazioni tecnologiche che si sono progressivamente registrate sono sempre state ad appannaggio esclusivo degli avvocati, i quali, del resto, ne sono sempre stati gelosi, per non rivelare i trucchi del mestiere ai loro clienti. Come è stato giustamente osservato, fino a un secolo fa «gli avvocati funzionavano come i sacerdoti medievali: detenevano informazioni a cui il pubblico non aveva accesso. Per la maggior parte, gli individui con domande legali dovevano rivolgersi agli avvocati, poiché nessun altro conosceva le risposte»¹⁸.

Le più recenti tecnologie, tuttavia, sembrano innescare una nuova fase di questa evoluzione. Ad esempio, la facilità con cui è possibile reperire informazioni su Internet sta gradualmente portando a una progressiva «volgarizzazione» dei formulari. Con Internet, chiunque ha libero accesso a modelli di documenti legali, in una più ampia «democratizzazione» dell'informazione, non solo giuridica¹⁹.

L'intelligenza artificiale generativa potrebbe compiere un ulteriore passo avanti in questa evoluzione. Finora la semplificazione del diritto è stata un ideale sostanzialmente irraggiungibile (anzi, un mito). Proprio per questo motivo, il ruolo della professione legale è sempre stato quello di rendere il diritto accessibile a coloro che non hanno le conoscenze tecniche per comprenderlo e

10. In generale, sulle origini delle norme sull'esercizio non autorizzato della professione forense, si veda AVERY-SANCHEZ ABRIL-DEL RIEGO 2023.

11. HAZARD-DONDI 2004; REMUS 2014, p. 1249, DONDI 2012, p. 867.

12. ABEL 2003; DEZALAY 1990; DEZALAY 1992; REMUS 2014, p. 1252.

13. CHAYES-CHAYES 1985; REGAN-ROHRER 2021; RIBSTEIN 2010; KAGAN-ROSEN 1985; WENDEL 2023; GALANTER-PALAY 1991.

14. REMUS 2014, p. 1256.

15. BARTON 2001.

16. JANSSEN-VENNMANN 2021, p. 46.

17. In generale, sull'influenza delle tecniche di documentazione sul diritto, si veda VISMANN 2008, p. 49.

18. AVERY-SANCHEZ ABRIL-DEL RIEGO 2023, p. 103.

19. GARAPON-LASSÈGUE 2018, p. 95; AVERY-SANCHEZ ABRIL-DEL RIEGO 2023, p. 103. In generale, anche per ulteriori riferimenti, si veda ASHLEY 2017, p. 234; SUSSKIND-SUSSKIND 2015, p. 231; REMUS-LEVY 2017, p. 501.

applicarne i formalismi. Tuttavia, gli strumenti di IA generativa, proprio perché in grado di rispondere nel linguaggio comune, potrebbero superare anche quest'ultimo ostacolo²⁰. In particolare, l'avvento dell'IA generativa potrebbe essere definito come una vera e propria seconda ondata di trasformazione digitale²¹.

Certamente, questo non è mai accaduto nel caso delle tecnologie progressivamente utilizzate dagli avvocati; fino ad oggi, le nuove tecnologie sono state solo strumenti di ausilio all'avvocato, e quindi è sempre stato l'avvocato a decidere se e come utilizzarle; ed è sempre stato l'avvocato ad esserne responsabile. Questo ragionamento, tuttavia, non sembra più valido nel caso di strumenti basati sull'IA generativa, proprio perché possono essere utilizzati da tutti, anche senza l'assistenza di un avvocato²². Si può addirittura immaginare, nelle giurisdizioni in cui è ammessa la difesa personale, che la parte possa farsi rappresentare dall'IA²³. Del resto, secondo le norme internazionali (ad esempio l'art. 6 della CEDU) e i principi del giusto processo (ad esempio la decisione *Gideon* negli Stati Uniti²⁴), la difesa tecnica è un diritto fondamentale, ma non è un dovere; in realtà, in molte giurisdizioni la difesa personale è assai limitata. Per queste ragioni, al netto di una specifica autorizzazione normativa, è assai difficile immaginare l'uso dell'intelligenza artificiale al posto di un avvocato nella rappresentanza giudiziale²⁵.

Ben più realistica, invece, è la possibilità che, in pochissimi anni, l'IA venga utilizzata per offrire consulenza legale extragiudiziale o per attività collaterali al processo²⁶. In effetti, i sempre più diffusi strumenti tecnologici in grado di fornire un'assistenza legale automatizzata alle persone hanno il potenziale per sostituire o almeno competere con l'assistenza legale tradizionale. Già oggi esistono molti strumenti di questo tipo²⁷ negli Stati Uniti²⁸, in America Latina²⁹, in Asia³⁰ e in Europa³¹.

Apparentemente, il problema non sembra differire dalla presenza, già assai diffusa, di modelli di documenti legali attualmente disponibili su Internet. Infatti, si potrebbe pensare che chiunque sappia che un modello di documento trovato su Internet non è di per sé affidabile o immediatamente utilizzabile. Tuttavia, questa percezione potrebbe svanire nel caso di strumenti basati sull'IA generativa i quali, utilizzando il linguaggio di elaborazione naturale (NPL), possono essere addestrati a fornire consulenza legale automatizzata³². Non sembra irragionevole parlare di veri e propri "formulari intelligenti", cioè di formulari che, parafrasando una bella espressione usata da Antoine Garapon e Jean Lassègue, "parlano da soli"³³.

In questo caso, è più facile che l'utente consideri affidabili i consigli forniti dallo strumento di IA che lo ha guidato passo dopo passo nel processo di compilazione. In altre parole, c'è il serio rischio che, attraverso l'IA generativa, si verifichi una sorta di esercizio non autorizzato della professione

20. TRANCOSO–MAMEDE–MARTINS et al. 2024.

21. RODRÍGUEZ DE LAS HERAS BALLELL 2019, p. 303.

22. GROSSMAN–GRIMM–BROWN–XU 2021.

23. GUNDER 2014, pp. 363, 403, PRESCOTT 2017; GLOVER 2016, GROSSMAN–GRIMM–BROWN–XU 2021, p. 66, NIEVA FENOLL 2022.

24. *Gideon v. Wainwright*, 372 U.S. 335, 343 (1963). Su questo tema, si veda WOO–COX–ROSEN 2022.

25. GASCÓN INCHAUSTI 2022, p. 3.

26. DAVIS 2022, p. 1190, GASCÓN INCHAUSTI 2022, p. 44.

27. CASERTA–MADSEN 2019, p. 8.

28. ENGSTROM–ENGSTROM 2023, p. 133, BARTON 2023, p. 23.

29. A questo proposito, si vedano i vari articoli pubblicati nel numero monografico, dedicato a *Legaltech*, della *Informática y Derecho*, *Revista Iberoamericana de Derecho Informático*, 2019, n. 7.

30. ZUO 2018, YAO 2019.

31. HARTUNG–BUES–HALBLEIB 2018, p. 7, JANSSEN–VENNMANN 2021, p. 50, BIARD 2019, p. 167, BARRIO ANDRÉS 2019, p. 37, MASSARO 2023, p. 99.

32. DAVIS 2022, p. 1188, FRANKENREITER–NYARKO 2023, p. 70.

33. GARAPON–LASSÈGUE 2018; BARTON 2023, p. 37 e PHELPS–ASHLEY 2022.

forense (*Unauthorised Practice of Law*, secondo la terminologia ampiamente diffusa negli ordinamenti anglosassoni) e la nascita di un mercato di servizi di consulenza legale³⁴. Esistono già molte aziende (i cosiddetti *Alternative Legal Services Providers* o *Legal Tech companies*) che offrono e forniscono servizi di consulenza legale basati sull'IA³⁵. Pertanto, non sembra irragionevole prevedere una possibile “uberizzazione” delle professioni legali³⁶. In altre parole, oggi il monopolio che l'avvocatura ha avuto finora è a rischio³⁷.

3. Il tramonto del monopolio degli avvocati?

È quindi necessario chiedersi se i servizi legali forniti dalle società di Legal Tech possano essere considerati come esercizio non autorizzato della professione forense. La questione non è semplice. Non lo è, innanzitutto, perché è difficile capire cosa significhi esercizio della professione forense³⁸. In generale, gli avvocati hanno il monopolio della fornitura di servizi legali dentro e fuori dal

tribunale³⁹. Non è sempre chiara, tuttavia, la portata di questo monopolio. In alcuni ordinamenti, la legge indica espressamente le attività riservate all'avvocato, come ad esempio in Germania⁴⁰. In altri, invece, la legge riserva genericamente la consulenza legale agli avvocati, senza definire cosa si intenda per consulenza legale⁴¹.

In secondo luogo, appare difficile applicare le norme sull'esercizio non autorizzato della professione forense all'IA⁴². Ad esempio, è complicato determinare se una particolare tecnologia sia assimilabile all'attività di mera trascrizione delle informazioni fornite da un cliente (non costituendo quindi esercizio non autorizzato della professione) oppure alla vera e propria attività di selezione e compilazione di un atto giuridico (costituendo quindi esercizio non autorizzato della professione)⁴³.

Ad esempio, nel caso *Janson v. LegalZoom.com, Inc.*⁴⁴, un'azione collettiva presentata presso la Corte del Distretto Occidentale del Missouri, il tribunale ha stabilito che non vi è alcuna differenza

34. SIMSHAW 2022, REMUS-LEVY 2017.

35. JIANG-DI MATTEO-THOMAS 2021, HELLWIG-EWER 2020, pp. 1783, 1784. VAN VEENEN-SCHMAAL 2018, p. 77.

36. TARNAUD-BOURGEOIS-BABIN 2018, YAO 2019, p. 483, SIMSHAW 2022, p. 165. YOON 2016, p. 456, SUÁREZ XAVIER 2022.

37. GARAPON-LASSÈGUE 2018, p. 97, REMUS-LEVY 2017, p. 504, CASERTA-MADSEN 2019, p. 10.

38. REMUS 2014, p. 1261, la quale osserva che nel 2003 un comitato dell'ABA ha fallito nel tentativo di promulgare un modello di definizione uniforme della pratica legale.

39. BARTON 2023, p. 22, secondo il quale, benché la definizione di “esercizio della professione forense” e i livelli di applicazione varino da Stato a Stato, come minimo in nessuno Stato un non avvocato può comparire in tribunale per conto di un'altra parte o fornire “consulenza legale”. RHODE 1981.

40. In Germania i servizi legali extragiudiziali sono regolati dal par. 2 della legge sui servizi legali (*Rechtsdienstleistungsgesetz/RDG*). L'RDG consiste in un elenco di divieti legali soggetti ad autorizzazione, il che significa che i servizi legali extragiudiziali sono generalmente vietati a meno che non siano espressamente autorizzati (par. 3 RDG). WIESIKE 2023, pp. 201, 203.

41. È il caso, ad esempio, di Italia, dove l'articolo 2 della legge 31 dicembre 2012, n. 247 (la disciplina italiana della professione forense) prevede che l'attività professionale di consulenza e assistenza legale stragiudiziale sia riservata agli avvocati solo se connessa all'attività giudiziaria; se svolta in modo continuativo, sistematico e organizzato, è di competenza degli avvocati. Si veda anche in Francia l'articolo 4 della legge n. 71-1130 del 31 dicembre 1971 (*portant réforme de certaines professions judiciaires et juridiques*), che riserva espressamente agli avvocati solo la difesa in giudizio; si veda TARNAUD-BOURGEOIS-BABIN 2018, p. 108.

42. SIMSHAW 2022, p. 215.

43. REMUS-LEVY 2017, p. 542.

44. *Janson v. Legalzoom.com, Inc.*, 802 F. Supp.2d 1053 (W.D. Mo. 2011). Anche un'altra società statunitense di tecnologia legale (DoNotPay) è stata citata in giudizio in diverse azioni per pratica legale non autorizzata (ad esempio, *Faridian v. DoNotPay, Inc.* e *MillerKing, LLC v. DoNotPay, Inc.*) raggiungendo in seguito un accordo, v. CASSENS WEISS 2024.

sostanziale tra un avvocato che prepara un documento per un cliente e i servizi forniti da LegalZoom. Di conseguenza, a LegalZoom è stato chiesto di interrompere l'offerta di questi servizi. Questa decisione è stata presa nonostante il disclaimer completo di LegalZoom, presentato a tutti i clienti⁴⁵.

In senso opposto, il 27 novembre 2019, la Corte federale di giustizia tedesca (*Bundesgerichtshof*, BGH), adottando un'interpretazione ampia dei "servizi di riscossione", ha ritenuto che i servizi forniti dalla società *Lexfox*, registrata come fornitore di servizi legali per i servizi di riscossione, non violassero la legge tedesca sui servizi legali (*Rechtsdienstleistungsgesetz*/RDG). Tuttavia, in questa decisione la Corte ha affermato che la questione se una determinata attività di un fornitore di servizi di riscossione registrato violi la legge sui servizi legali deve essere risolta caso per caso⁴⁶.

Infatti, se si intende per pratica del diritto anche l'analisi di leggi e regolamenti al fine di verificare l'applicabilità di una determinata legge a un caso specifico, come sostenuto dalla Corte di Cassazione francese (anche se non con specifico riferimento al caso IA), allora i servizi offerti dai fornitori di servizi Legal Tech dovrebbero essere considerati attività legale⁴⁷.

In terzo luogo, l'uso delle norme UPL (relative, cioè, all'*Unauthorized Practice of Law*) potrebbe non essere socialmente accettato. Infatti, le azioni legali UPL sembrano spesso motivate da un interesse personale da parte della professione legale, che mira a salvaguardare il proprio dominio esclusivo. Queste azioni legali sono spesso percepite

come tentativi da parte dell'ordine degli avvocati di mantenere il monopolio sui servizi legali, impedendo la concorrenza dei non avvocati che potrebbero offrire soluzioni più convenienti o innovative. I critici sostengono che tali azioni legali non mirano tanto a proteggere il pubblico da professionisti non qualificati, quanto piuttosto a preservare gli interessi economici e il controllo dell'establishment legale⁴⁸.

Alcuni sostengono addirittura che le norme UPL dovrebbero essere abrogate⁴⁹. Anche senza arrivare a una soluzione così estrema, tuttavia, sembra chiaro che queste norme non sono oggi adeguate per far fronte all'uso dell'IA nella fornitura di servizi legali.

4. Legal Tech e AI Act: necessità di una regolamentazione *ad hoc* per la consulenza legale online?

La difficoltà di applicare le norme sull'esercizio abusivo della professione legale solleva un'altra questione: la legge deve prevedere una specifica regolamentazione per la consulenza legale online⁵⁰? E deve imporre specifici requisiti di affidabilità per l'uso dell'IA generativa⁵¹?

Anche in questo caso, non è facile rispondere a queste domande. Ad esempio, il regolamento UE sull'intelligenza artificiale (AI Act) non sembra tenere conto di questa situazione, in quanto non considera l'uso dell'intelligenza artificiale per la consulenza legale come un'attività ad alto rischio⁵². Infatti, secondo questo regolamento, gli strumenti che offrono consulenza legale basata sull'intelligenza artificiale non sembrano rientrare

45. Su questo caso, cfr. AVERY-SANCHEZ ABRIL-DEL RIEGO 2023, p. 91.

46. *Bundesgerichtshof*, BGH 27 novembre 2019, in "Neue Juristische Wochenschrift", 2020, 208. Su questo caso, si veda HOCH-LOY-HENDRICKS 2020, pp. 254, 256; LEEB 2020.

47. MASSART 2023, p. 16.

48. REMUS-LEVY 2017, p. 542.

49. AVERY-SANCHEZ ABRIL-DEL RIEGO 2023, pp. 101 e 128, i quali ritengono che il mantenimento dello *status quo* dell'UPL non sia più sostenibile e la prova inconfutabile che la giustizia non è uguale secondo la legge e che il monopolio degli avvocati non promuove il bene pubblico. Su questo tema, si veda anche SEN 2019, p. 121; RHODE-CUMMINGS 2017, p. 490; RIGERTAS 2014.

50. Sul problema della regolamentazione dell'IA in generale, si veda BUENO DE MATA 2022, p. 15; MANTELERO 2022, p. 140.

51. REMUS-LEVY 2017, p. 545; SIMSHAW 2022, p. 156; CASERTA-MADSEN 2019, p. 14.

52. Si veda, in generale, sull'approccio basato sul rischio del regolamento europeo, PAUL 2023; LAUX-WACHTER-MITTELSTADT 2024.

in un settore ad alto rischio. In particolare, il regolamento considera ad alto rischio solo i sistemi di IA «destinati a essere utilizzati da un'autorità giudiziaria o per suo conto per assistere un'autorità giudiziaria», escludendo quindi implicitamente dal campo di applicazione gli strumenti utilizzati al di fuori dell'attività giudiziaria⁵³.

Questo approccio non sembra accettabile e può avere un impatto molto negativo sull'accesso alla giustizia⁵⁴. Si pensi, ad esempio, a una persona che riceve una consulenza da uno strumento basato sull'IA e, basandosi esclusivamente sulla soluzione fornita da questo strumento, decide di non intraprendere un'azione legale. Sembra francamente difficile immaginare che un tale uso di uno strumento di IA, che potenzialmente scoraggia l'accesso alla giustizia, non sia ad alto rischio⁵⁵.

Non dobbiamo nemmeno dimenticare i potenziali conflitti di interesse che potrebbero sorgere tra il proprietario-operatore dello strumento di consulenza legale e gli utenti. Possiamo ipotizzare uno strumento di IA generativa per la consulenza legale di proprietà di un'azienda che offra anche altri servizi ai consumatori: c'è ovviamente il rischio che la consulenza legale offerta sia finalizzata a scoraggiare potenziali azioni legali contro tale e-commerce o fornitore di servizi; inoltre, in assenza di regolamentazione, questo rischio potrebbe aumentare a causa dell'asimmetria informativa tra le parti⁵⁶ e del fatto che gli algoritmi predittivi finirebbero quasi certamente nelle mani di pochissime grandi aziende⁵⁷.

In questo caso è molto più difficile che gli utenti si rendano conto del conflitto di interessi; è stato giustamente osservato che quando i servizi legali sono forniti in modo impersonale, senza interazione umana, è improbabile che i casi di rappresentanza in conflitto suscitino gli stessi sentimenti di tradimento che si avrebbero se fosse coinvolto un avvocato umano⁵⁸.

Questi algoritmi inaffidabili potrebbero anche influenzare negativamente i giudici e gli avvocati che, pur non essendo autorizzati a farlo, potrebbero comunque essere tentati di utilizzare segretamente tali algoritmi per mere ragioni di convenienza, per semplificare il loro lavoro. Dopo tutto, le previsioni sono molto comode da usare e possono influenzare il comportamento umano⁵⁹.

Ma potrebbero esserci ulteriori problemi, sempre per quanto riguarda l'accesso alla giustizia. Potrebbe crearsi un nuovo divario tecnologico tra ricchi e poveri⁶⁰. In sostanza, c'è il rischio di un sistema giudiziario a due livelli, con avvocati umani costosi – ma superiori – e un'assistenza legale guidata dall'IA poco costosa – ma inferiore⁶¹. In realtà, l'IA (che apparentemente diminuirebbe i divari tra ricchi e poveri) potrebbe anche esacerbarli⁶².

Ma immaginiamo anche che non sia così. Si può ipotizzare che l'uso di strumenti di IA generativa possa facilitare l'accesso alla giustizia. È stato osservato che l'analisi statistica delle sentenze potrebbe aiutarci a comprendere meglio le tendenze chiave del processo decisionale giudiziario, a identificare

53. Si veda l'Allegato III del Regolamento UE n. 1689/2024 (Legge sull'IA). Lo stesso approccio sembra essere seguito in Cina, dove la proposta di regolamentazione dell'IA riguarda solo le domande presentate alla Corte: si veda l'articolo 70 (attività giudiziaria) della legge sull'intelligenza artificiale della Repubblica popolare cinese (bozza per i suggerimenti degli studiosi).

54. HYDE 2023, p. 1276.

55. LEBRETON-DERRIEN 2018, p. 13, il quale afferma giustamente che «La justice prédictive devient instrument de dissuasion et un tel évitement du procès ne peut évidemment être accepté s'il conduit à restreindre l'accès du justiciable au juge».

56. ENGSTROM-ENGSTROM 2023, p. 147, secondo i quali solo le parti abituali possono fare affidamento sull'accesso privilegiato ai dati riservati di liquidazione dei sinistri per addestrare il proprio algoritmo.

57. FILIOL 2018, p. 151, ponendo, più in generale, il rischio di una perdita di sovranità degli Stati.

58. BRIMO 2022, p. 570.

59. ENGSTROM-GELBACH 2021, p. 1036; GABELLINI 2019, p. 1305.

60. REMUS-LEVY 2017, p. 545; ENGSTROM-GELBACH 2021, p. 1038.

61. SIMSHAW 2022, p. 156.

62. ENGSTROM-GELBACH 2021, p. 1072; WOO-COX-ROSEN 2022, p. 1114.

le distorsioni dei tribunali e a individuare le pratiche anomale. Ciò potrebbe ridurre i costi legali e, in ultima analisi, migliorare l'accesso alla giustizia⁶³. Inoltre, gli strumenti basati sull'IA generativa potrebbero effettivamente rendere la giustizia più accessibile, migliorando l'assistenza legale⁶⁴.

Anche se fosse così, sorgono altri problemi. Innanzitutto, c'è un problema di trasparenza degli algoritmi. L'opacità degli strumenti di IA rende difficile valutarne l'affidabilità⁶⁵. Infatti, come è stato giustamente osservato, la tecnologia può essere resa opaca per proteggere un investimento, ma anche per evitare un controllo; tale controllo può rivelare segreti commerciali, oppure può rivelare incompetenza⁶⁶.

Se l'attività di consulenza legale svolta dalle società di *legal tech* non costituisse attività forense, pur se lecita e non lesiva dell'accesso alla giustizia, allora si dovrebbe comunque escludere l'applicabilità delle norme deontologiche e del dovere di riservatezza⁶⁷.

Infine, si pone un problema di responsabilità. Chi è responsabile se il contenuto generato dall'IA non è corretto⁶⁸? In genere, nel caso degli avvocati, la legge impone quasi sempre un obbligo di assicurazione. Tali obblighi, tuttavia, non possono essere automaticamente estesi alle società di *legal tech* e, pertanto, sarebbe necessaria una norma giuridica specifica che imponga l'obbligo di assicurazione⁶⁹.

Ovviamente, la questione della trasparenza degli algoritmi è troppo complessa per essere affrontata in questa sede. Tuttavia, in conclusione, sembra inevitabile auspicare l'adozione di una normativa *ad hoc* che imponga requisiti specifici di affidabilità per gli strumenti di IA generativa che offrano consulenza legale. E ciò pur con la consapevolezza che questo non risolverebbe comunque tutti i problemi, primo fra tutti quello di decidere quale grado di trasparenza e spiegabilità deve essere garantito⁷⁰.

Riferimenti bibliografici

- R. ABEL (2003), *English Lawyers between the Market and the State. The Politics of Professionalism*, Oxford University Press, 2003
- T. ASAI (2011), *The Image of the Lawyer in Modern China*, in S. Fuma, "Research of China litigation social history", Kyoto University Press, 2011
- K.D. ASHLEY (2017), *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age*, Cambridge University Press, 2017
- J.J. AVERY, P. SANCHEZ ABRIL, A. DEL RIEGO (2023), *ChatGPT, Esq.: Recasting Unauthorized Practice of Law in the Era of Generative AI*, in "Yale Journal of Law and Technology", vol. 26, 2023, n. 1
- M. BARRIO ANDRÉS (dir.) (2019), *Legal Tech. La transformación digital de la abogacía*, Wolters Kluwer, 2019
- B.H. BARTON (2023), *The Future of American Legal Tech: Regulation, Culture, Markets*, in D.F. Engstrom (dir.), "Legal Tech and the Future of Civil Justice", Cambridge University Press, 2023

63. JANEČEK 2023; FERRARI-MUSTARI 2023, p. 124.

64. BARTON-RHODE 2019, p. 956; GILLERS 2012; MEDIANIK 2018, p. 1498.

65. MOURIESSE 2018.

66. CHESTERMAN 2021, p. 271.

67. BRIMO 2022, p. 561; WALTERS 2019, p. 1079.

68. BRIMO 2022, p. 573.

69. AVERY-SANCHEZ ABRIL-DEL RIEGO 2023, p. 127.

70. BROŽEK-FURMAN-JAKUBIEC-KUCHARZYK 2023. In questo senso, con riferimento alle piattaforme che offrono servizi ODR; BIARD 2019, p. 174.

- B.H. BARTON (2001), *Why Do We Regulate Lawyers? An Economic Analysis of the Justifications for Entry and Conduct Regulation*, in “Arizona State Law Journal”, vol. 33, 2001, n. 2
- B.H. BARTON, D.L. RHODE (2019), *Access to Justice and Routine Legal Services: New Technologies Meet Bar Regulators*, in “Hastings Law Journal”, vol. 70, 2019, n. 4
- A. BIARD (2019), *Justice en ligne ou nouveau Far Www.est? La difficile régulation des plateformes en ligne de règlement extrajudiciaire des litiges*, in “Revue internationale de droit économique”, 2019, n. 2
- B.K. BRIMO (2022), *How Should Legal Ethics Rules Apply When Artificial Intelligence Assists Pro Se Litigants?*, in “Georgetown Journal of Legal Ethics”, vol. 35, 2022, n. 4
- B. BROŻEK, M. FURMAN, M. JAKUBIEC, B. KUCHARZYK (2023), *The black box problem revisited. Real and imaginary challenges for automated legal decision making*, in “AI & Law”, vol. 32, 2023
- F. BUENO DE MATA (2022), *La necesidad de regular la inteligencia artificial y su impacto como tecnología disruptiva en el proceso: de desafío utópico a cuestión de urgente necesidad*, in F. Bueno De Mata (coord.), “El impacto de las tecnologías disruptivas en el Derecho procesal”, Thomson Reuters Aranzadi, 2022
- S. CASERTA, M. MADSEN (2019), *The Legal Profession in the Era of Digital Capitalism: Disruption or New Dawn?*, in “Laws”, vol. 8, 2019, n. 1
- D. CASSENS WEISS (2024), *‘Robot lawyer’ DoNotPay reaches settlement in suit alleging it’s neither robot nor lawyer*, in “Aba Journal”, 11 June 2024
- A. CHAYES, A.H. CHAYES (1985), *Corporate Counsel and the Elite Law Firm*, in “Stanford Law Review”, vol. 37, 1985, n. 2
- S. CHESTERMAN (2021), *Through a Glass, Darkly: Artificial Intelligence and the Problem of Opacity*, in “American Journal of Comparative Law”, vol. 69, 2021, n. 2
- P. COMOGLIO (2022), *Il processo come fenomeno economico di massa. Problemi di finanziamento e di remunerazione delle controversie civili*, Giappichelli, 2022
- J.P. DAVIS (2022), *Of Robolawyers and Robojudges*, in “Hastings Law Journal”, vol. 73, 2022, n. 5
- E.A. DAVIS (2003), *The Meaning of Professional Independence*, in “Columbia Law Review”, vol. 103, 2003, n. 5
- B. DEFFAINS (2023), *L’avocat et le marché: une perspective économique*, in “Archives de philosophie du droit”, vol. 64, 2023, n. 1
- Y. DEZALAY (1992), *Marchands de droit. La restructuration de l’ordre juridique international par les multinationals du droit*, Fayard, 1992
- Y. DEZALAY (1990), *The Big Bang and the Law: The Internationalization and Restructuration of the Legal Field*, in “Theory, Culture & Society”, vol. 7, 1990, n. 2-3
- A. DONDI (2012), *Conduite de l’avocat et loyauté procédurale. Une tentative de mise à jour*, in J.-Y. Chérot (ed.), “Mélanges en l’honneur de Jean-Louis Bergel”, Bruylant, 2012
- A. DONDI, V. ANSANELLI, P. COMOGLIO (2017), *Procesos civiles en evolución. Una perspectiva comparada*, Marcial Pons, 2017
- D.F. ENGSTROM, N.F. ENGSTROM (2023), *Legal Tech and the Litigation Playing Field*, in D.F. Engstrom (dir.), “Legal Tech and the Future of Civil Justice”, Cambridge University Press, 2023
- D.F. ENGSTROM, J.B. GELBACH (2021), *Legal Tech, Civil Procedure, and the Future of Adversarialism*, in “University of Pennsylvania Law Review”, vol. 169, 2021
- F. FERRARI, D. MUSTARI (2023), *The New Technologies and the Civil Justice as Commons*, in “Revista Ítalo-Española de Derecho Procesal”, 2023, n. 1

- E. FILIOL (2018), *Les risques concernant l'utilisation des algorithmes dits prédictifs dans le domaine sensible de la justice*, in "Archives de philosophie du droit", vol. 60, 2018, n. 1
- J. FRANKENREITER, J. NYARKO (2023), *Natural Language Processing in Legal Tech*, in D.F. Engstrom (dir.), "Legal Tech and the Future of Civil Justice", Cambridge University Press, 2023
- E. GABELLINI (2019), *La "comodità nel giudicare": la decisione robotica*, in "Rivista trimestrale di diritto e procedura civile", 2019, n. 4
- M. GALANTER, T. PALAY (1991), *Tournament of Lawyers: The Transformation of the Big Law Firm*, University of Chicago Press, 1991
- A. GARAPON, J. LASSÈGUE (2018), *Justice digitale*, PUF, 2018
- F. GASCÓN INCHAUSTI (2022), *Eficiencia procesal y sistemas de inteligencia artificial: la necesidad de pasar a la acción normativa*, in F. Ordóñez Ponz, S.F. Rodríguez Ríos (eds.), "Modernización, eficiencia y aceleración del proceso", Aranzadi, 2022
- S. GILLERS (2012), *A Profession, If You Can Keep It: How Information Technology and Fading Borders Are Reshaping the Law Marketplace and What We Should Do About It*, in "Hastings Law Journal", vol. 63, 2012, n. 4
- G.J. GLOVER (2016), *Online Legal Service Platforms and the Path to Access to Justice*, in "Florida Bar Journal", vol. 90, 2016
- M.R. GROSSMAN, P.W. GRIMM, D.G. BROWN, M. XU (2023), *The GPTJudge: Justice in a Generative AI World*, in "Duke Law & Tech Review", vol. 23, 2023, n. 1
- J.R. GUNDER (2014), *Why Can't I Have a Robot Lawyer? Limits on the Right to Appear Pro Se*, in "Tulane Law Review", vol. 98, 2014, n. 3
- M. HARTUNG, M. BUES, G. HALBLEIB (2018), *Legal Tech. How Technology is Changing the Legal World: a Practitioner's Guide*, Beck, 2018
- G.C. HAZARD, A. DONDI (2006), *Responsibilities of Judges and Advocates in Civil and Common Law: Some Lingerin Misconceptions Concerning Civil Lawsuits*, in "Cornell International Law Journal", vol. 39, 2006
- G.C. HAZARD, A. DONDI (2004), *Legal Ethics, A comparative Study*, Stanford University Press, 2004
- G.C. HAZARD, A. DONDI (2001), *A Short Historical Sketch of the Legal Professions*, in "Zeitschrift für Zivilprozess International: Jahrbuch des Internationalen Zivilprozessrechts", 2001
- H. HELLWIG, W. EWER (2020), *Keine Angst vor Legal Tech*, in "Neue Juristische Wochenschrift", 2020
- V. HOCH-LOY, J.D. HENDRICKS (2020), *Das RDG und die Legal Tech-Debatte: Und wo bleibt das Unionsrecht?*, in "Verbraucher und Recht", vol. 35, 2020, n. 7
- A. HYDE (2023), *Plaidoyer pour l'inclusion des outils de jurimétrie dans le futur règlement européen sur l'intelligence artificielle*, in "La semaine juridique", 2023, n. 39
- V. JANEČEK (2023), *Judgments as bulk data*, in "Big Data & Society", vol. 10, 2023, n. 1
- A. JANSSEN, T.J. VENNMANN (2021), *The Effects of Technology on Legal Practice. From Punch Card to Artificial Intelligence?*, in L.A. Di Matteo, A. Janssen, P. Ortolani et al. (eds.), "The Cambridge Handbook of Lawyering in the Digital Age", Cambridge University Press, 2021
- J.C. JIANG, L.A. DI MATTEO, R.E. THOMAS (2021), *Disruptive Effects of Legal Tech*, in L.A. Di Matteo, A. Janssen, P. Ortolani et al. (eds.), "The Cambridge Handbook of Lawyering in the Digital Age", Cambridge University Press, 2021

- R.A. KAGAN, R.E. ROSEN (1985), *On the Social Significance of Large Law Firm Practice*, in “Stanford Law Review”, vol. 37, 1985, n. 2
- I. KITAMURA (2023), *L'avocat dans la culture japonaise*, in “Archives de Philosophie du Droit”, vol. 64, 2023, n. 1
- J. LAUX, S. WACHTER, B. MITTELSTADT (2024), *Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk*, in “Regulation & Governance”, vol. 18, 2024, n. 1
- S. LEBRETON-DERRIEN (2018), *La justice prédictive. Introduction à une justice «simplement» virtuelle*, in “Archives de Philosophie du Droit”, vol. 60, 2018, n. 1
- C.-M. LEEB (2020), *Update Legal Tech: So entscheiden Deutschlands Gerichte*, 3 August 2020
- D. LUBAN (1988), *Lawyers and Justice. An Ethical Study*, Princeton University Press, 1988
- A. MANTELERO (2022), *Beyond Data Human Rights, Ethical and Social Impact Assessment in AI*, Springer, 2022
- M. MASSARO (2023), *Le réseau des projets LegalTechs en Belgique. Entre innovations techniques et avocats-entrepreneurs du droit*, in “Sociologies pratiques”, vol. 46, 2023, n. 1
- T. MASSART (2023), *Les avocats confrontés à l'intelligence artificielle*, in “Revue Pratique de la Prospective et de l'Innovation”, 2023, n. 1
- K. MEDIANIK (2018), *Artificially Intelligent Lawyers: Updating the Model Rules of Professional Conduct in Accordance with the New Technological Era*, in “Cardozo Law Review”, vol. 39, 2018, n. 4
- K. MIYAGAWA, K. NASU, M. KOYAMA, H. KUBORI (1992) (dir.), *Henkaku no naka no bengoshi: sono rinen to jissen* (Avvocati e riforma: idee e pratiche), Yūhikaku, 1992
- I. MIYATA (2021), *Gekihen suru bengoshi* (Avvocati e grandi cambiamenti), Tokyo Kyōei Shobō, 2021
- E. MOURIESSE (2018), *Quelle transparence pour les algorithmes de justice prédictive?*, in “Archives de philosophie du droit”, vol. 60, 2018
- J. NIEVA FENOLL (2022), *Technology and fundamental rights in the judicial process*, in “Civil Procedure Review”, vol. 13, 2022, n. 2
- F. ORDÓÑEZ PONZ, S.F. RODRÍGUEZ RÍOS (eds.) (2022), *Modernización, eficiencia y aceleración del proceso*, Aranzadi, 2022
- R. PAUL (2023), *European artificial intelligence “trusted throughout the world”: Risk-based regulation and the fashioning of a competitive common AI market*, in “Regulation & Governance”, vol. 18, 2023, n. 4
- T. PHELPS, K. ASHLEY (2022), *“Alexa, Write a Memo”: The Promise and Challenges of AI and Legal Writing*, in “Legal Writing”, vol. 26, 2022, n. 2
- J.J. PRESCOTT (2017), *Improving Access to Justice in State Courts with Platform Technology*, in “Vanderbilt Law Review”, vol. 70, 2017, n. 6
- M. REGAN, L.H. ROHRER (2021), *Biglaw: Money and Meaning in the Modern Law Firm*, University of Chicago Press, 2021
- D.A. REMUS (2017), *Reconstructing Professionalism*, in “Georgia Law Review”, vol. 51, 2017, n. 3
- D.A. REMUS (2014), *Out of Practice: The Twenty-First-Century Legal Profession*, in “Duke Law Journal”, vol. 63, 2014, n. 6
- D. REMUS, F. LEVY (2017), *Can Robots Be Lawyers: Computers, Lawyers, and the Practice of Law*, in “Georgetown Journal of Legal Ethics”, vol. 30, 2017, n. 3

- D. RHODE (ed.) (2000), *Ethics in Practice. Lawyers' Roles, Responsibility and Regulation*, Oxford University Press, 2000
- D.L. RHODE (1981), *Policing the Professional Monopoly: A Constitutional and Empirical Analysis of Unauthorized Practice Prohibitions*, in "Stanford Law Review", vol. 34, 1981
- D.L. RHODE, S.L. CUMMINGS (2017), *Access to Justice: Looking Back, Thinking Ahead*, in "Georgetown Journal of Legal Ethics", vol. 30, 2017, n. 3
- L.E. RIBSTEIN (2010), *The Death of Big Law*, in "Wisconsin Law Review", 2010, n. 3
- L.A. RIGERTAS (2014), *The Legal Profession's Monopoly: Failing to Protect Consumers*, in "Fordham Law Review", vol. 82, 2018, n. 6
- T. RODRÍGUEZ DE LAS HERAS BALLELL (2019), *Legal challenges of artificial intelligence: modelling the disruptive features of emerging technologies and assessing their possible legal impact*, in "Uniform Law Review", vol. 24, 2019, n. 2
- B. SEN (2019), *Beyond the JD: How eliminating the legal profession's monopoly on legal services can address the access-to-justice crisis*, in "University of Pennsylvania Journal of Law and Social Change", vol. 22, 2019, n. 3
- R. SÉVE (2023), *Avant-Propos: l'Avocature, de l'essence aux existences*, in "Archives de philosophie du droit", vol. 64, 2023
- D. SIMSHAW (2022), *Access to A.I. Justice: Avoiding an Inequitable Two-Tiered System of Legal Services*, in "Yale Journal of Law & Technology", vol. 24, 2022
- P.R. SUÁREZ XAVIER (2022), *Inteligencia artificial y uberización de la abogacía: ¿quien regulará al abogado robot o al robot del abogado?*, in "Revista General de Derecho Procesal", 2022, n. 58
- R. SUSSKIND, D. SUSSKIND (2015), *The future of the professions: how technology will transform the work of human experts*, Oxford University Press, 2015
- N. TARNAUD, C. BOURGEOIS, L. BABIN (2018), *Les professions réglementées à l'épreuve de l'ubérisation du droit : vers un monde sans avocat?*, in "Management & Sciences Sociales", n. 25, 2018
- I. TRANCOSO, N. MAMEDE, B. MARTINS et al. (2024), *The Impact of Language Technologies in the Legal Domain*, in H. Sousa Antunes, P.M. Freitas, A.L. Oliveira et al. (eds.), *"Multidisciplinary Perspectives on Artificial Intelligence and Law"*, Springer, 2024
- J. VAN VEENEN, J. SCHMAAL (2018), *Legal tech en de advocatuur*, in "Computerrecht", 2018, n. 54
- C. VISMANN (2008), *Files. Law and Media Technology*, Stanford University Press, 2008
- E. WALTERS (2019), *The Model Rules of Autonomous Conduct: Ethical Responsibilities of Lawyers and Artificial Intelligence*, in "Georgia State University Law Review", vol. 35, 2019, n. 4
- J. WANG (2019), *Achievements of China's Lawyer Profession in the Past 40 Years and Future Prospects*, in "Justice of China", 2019, n. 11
- W.B. WENDEL (2023), *Rumors of the Death of BigLaw Are Greatly Exaggerated Reviewing Mitt Regan & Lisa H. Rohrer, BigLaw: Money and Meaning in the Modern Law Firm (University of Chicago Press 2021)*, in "Georgetown Journal of Legal Ethics", vol. 36, 2023, n. 177
- O. WIESIKE (2023), *La profession d'avocat en Allemagne*, in "Archives de philosophie du droit", vol. 64, 2023
- M.Y.K. WOO, C. COX, S. ROSEN (2022), *Access to Civil Justice*, in "American Journal of Comparative Law", vol. 70, 2022, n. 1-s

- X. XU (2022), *Lawyers in Chinese Culture*, in “Archives de philosophie du droit”, vol. 64, 2022, n. 1
- Y. YAO (2019), *Uberizing the Legal Profession? Lawyer Autonomy and Status in the Digital Legal Market*, in “British Journal of Industrial Relations”, vol. 58, 2019, n. 3
- A.H. YOON (2016), *The Post-Modern Lawyer: Technology and the Democratization of Legal Representation*, in “University of Toronto Law Journal”, vol. 66, 2016, n. 4
- W.M. ZUO (2018), *Some thoughts on the application prospects of legal artificial intelligence in China*, in “Tsinghua University Law Journal”, 2018, n. 2



JACOPO DELLA TORRE – ALESSANDRO MALACARNE

Riforma Cartabia e digitalizzazione della giustizia penale

Il contributo offre una panoramica in merito alle principali novità apportate dalla l. n. 134/2021 e dal d.lgs. n. 150/2022 (cd. riforma Cartabia) sul versante della digitalizzazione del procedimento penale, mettendone in risalto pregi, difetti e lacune.

Diritti fondamentali – Digitalizzazione – Intelligenza artificiale – Processo penale telematico

Cartabia Reform and the digitalisation of the criminal justice system

The paper focuses on the main innovations introduced by Law 134/2021 and Legislative Decree 150/2022 (the so-called Cartabia reform) on the digitisation of criminal proceedings, highlighting their advantages, shortcomings and drawbacks.

Fundamental rights – Digitalisation – Artificial intelligence – Telematic criminal proceedings

J. Della Torre è ricercatore (RtdB) in Diritto processuale penale presso il Dipartimento di Giurisprudenza dell'Università di Genova

A. Malacarne è assegnista di ricerca in Diritto processuale penale presso il Dipartimento di Giurisprudenza dell'Università di Genova

Questo lavoro è stato parzialmente finanziato dal progetto NextGenerationEU “Security and Rights in CyberSpace” (SERICS) e dal progetto NextGenerationEU “Digitalization of the judiciary functions: trends, perspectives and risks” (PRIN PNRR, Codice progetto: P2022PRBCS, CUP D53D23022420001)

Il presente lavoro si inserisce nell'ambito del progetto, finanziato con fondi dell'Unione europea, *DigiRights – Digitalisation of defence Rights in criminal proceedings* (call JUST-2021-JACC, sovvenzione n. 101056667). Le opinioni e le osservazioni espresse nel testo sono riferibili esclusivamente agli Autori. Pur essendo il frutto di una riflessione congiunta, Jacopo Della Torre ha redatto i parr. 1, 3, 4, 4.1, 4.1.1, 4.1.2, 6, 8 e Alessandro Malacarne i parr. 2, 5, 7

Questo contributo fa parte della sezione monografica *Digitalizzazione del processo e diritti fondamentali – Profili processuali* a cura di Francesca Bailo e Michele Francaviglia

SOMMARIO: 1. Premessa: l'improcrastinabilità di una riforma sul versante della digitalizzazione del processo penale. – 2. Il disorganico quadro normativo previgente. – 3. Le novità apportate dalla riforma Cartabia. – 4. I pilastri del nuovo processo penale 2.0: l'atto nativo digitale, il fascicolo informatico e le novità in tema di verbalizzazione. – 4.1. *Il deposito telematico*. – 4.1.1. *Verso una nuova tipologia di invalidità processuale? L'"atto abilitante" e il concetto di "irricevibilità"*. – 4.1.2. *Il d.m. 29 dicembre 2023, n. 217 e la disciplina intertemporale e transitoria per i depositi*. – 5. Il nuovo applicativo ministeriale per la gestione del fascicolo telematico: cd. APP. – 6. Le notificazioni 2.0. – 7. La nuova disciplina organica della partecipazione a distanza. – 8. Auspici per il futuro.

1. Premessa: l'improcrastinabilità di una riforma sul versante della digitalizzazione del processo penale

Approvata onde rispettare gli impegni di riduzione dei tempi medi di trattazione dei procedimenti giudiziari (c.d. *disposition time*¹), così come assunti con le istituzioni europee nell'ambito del Piano Nazionale di Ripresa e Resilienza², la cd. riforma Cartabia (l. 27 settembre 2021, n. 134 e d.lgs. 10 ottobre 2022, n. 150)³ rappresenta, senza dubbio, una delle manovre più ambiziose e articolate che hanno interessato il sistema penale italiano negli ultimi trentacinque anni⁴.

Lo spirito profondamente innovativo che caratterizza vari settori della novella ben si coglie dallo studio di quello che costituisce uno dei suoi pilastri principali: l'aver cercato di favorire la transizione da una giustizia criminale ancora prevalentemente

analogica a una *digital-oriented*, perché volta ad attribuire un ruolo primario, in tutte le fasi del rito, alle *information and communications technology* (ICT)⁵.

Va da subito detto che il fatto che il legislatore abbia puntato sull'informatizzazione delle procedure giudiziarie non può stupire. Onde rendersi conto di ciò, è sufficiente richiamare le ormai numerose fonti sovranazionali che, dagli inizi del nuovo millennio, hanno incentivato gli ordinamenti interni ad adottare veri e propri modelli di *cyberjustice*. Tra queste meritano di essere segnalate, in particolare, le indicazioni provenienti dalla *European Commission for the Efficiency of Justice* (CEPEJ) – specie con riguardo all'utilizzo delle *Information Technology in European Courts*⁶ – che, con cadenza biennale⁷, elabora reports sulla qualità dei sistemi di giustizia penale in Europa; nonché, più di recente, gli spunti contenuti nelle *relazioni*

1. Si tratta dell'indicatore impiegato, a livello internazionale, per stimare la durata media dei procedimenti giudiziari. Esso misura il tempo necessario a smaltire, a flussi di definizione invariati, gli affari pendenti di un ufficio giudiziario alla fine di un determinato periodo di tempo.

2. L'impegno di ridurre del 25% tale parametro, entro il 2026, compare nell'allegato al PNRR, p. 372.

3. Per una sintesi dell'intervento, v., tra i molti, CANZIO 2021; DONINI 2021; GATTA 2021; LA ROCCA 2021; GIALUZ-DELLA TORRE 2022; SPANGHER 2021.

4. Tanto che AMODIO 2022, p. 7 l'ha paragonata a «una seconda delega dopo quella che nel 1987 ha dato avvio alla nascita del nuovo codice di procedura penale».

5. GALGANI 2022; CURTOTTI-NOCERINO 2024; DELVECCHIO 2021; SIGNORATO 2023.

6. CEPEJ, *Thematic report: Use of information technology in European courts*.

7. Da ultimo, ID., *Evaluation of judicial systems*. Report published on 5th October 2022.

del Fondo Monetario Internazionale⁸ e nell'*EU Justice Scoreboard*⁹.

L'analisi di questi (e di altri¹⁰) atti consente di porre in rilievo un aspetto chiave del rapporto che intercorre tra l'innovazione tecnologica e il procedimento penale. Si allude, più in dettaglio, alla circostanza per cui l'impiego di strumentazioni *paperless* è in grado di incidere positivamente sulla qualità e sulla funzionalità dell'intero apparato giudiziario. È ormai largamente dimostrata, del resto, l'idea per cui dall'accoglimento di una «nuova cultura “digitalocentrica”» possano «derivare benéfici effetti di “sistema”, garantendo un'architettura processuale più agile e snella per tutte le parti in gioco»¹¹. In effetti, una più coerente e organica informatizzazione delle attività procedurali, pure di natura organizzativa, consente, al contempo, di ridurre gli sprechi, velocizzare la macchina giudiziaria e incrementare le salvaguardie dei soggetti coinvolti nella vicenda penale. Tenuto conto di ciò, ben si comprende il perché si sia autorevolmente osservato che proprio sulla riuscita della svolta digitale «si fondano in buona parte le speranze di recuperare la ragionevole durata del processo»¹² perseguite dal riformatore.

A conferma di quanto appena detto soccorre pure il recente 2022–2025 *CEPEJ Action plan: Digitalisation for a better justice*¹³, ove si sottolinea la necessità che gli uffici giudiziari utilizzino le «information technology to optimise its operations, as well as the interconnection links between the various judicial institutions». Di talché, ben si comprende come la digitalizzazione delle procedure vada ricompresa tra i fattori in grado di contribuire allo sviluppo di una giustizia penale «efficiente»; concetto, quest'ultimo, che, come si è

sottolineato altrove, lungi dal dover essere inteso in senso squisitamente “produttivo”, assume, in un sistema con risorse limitate, le «vesti di criterio interpretativo implicito, rivolto a tutti i formanti dell'ordinamento, il quale impone agli stessi di optare per quelle soluzioni normative, esegetiche e/o strutturali, che permettono di raggiungere gli scopi prefissati dalle fonti sovraordinate, in modo qualitativamente ed economicamente appropriato, cioè minimizzando gli sprechi»¹⁴.

Se ciò è vero, va tuttavia rammentato che, come risaputo, fino all'approvazione della recente riforma, le potenzialità offerte dal progresso tecnologico erano state sfruttate solo in minima parte dal sistema penale italiano. Onde rendersi conto di ciò, è sufficiente ricordare come l'arretratezza della normativa e delle infrastrutture degli uffici italiani fosse stata denunciata, in modo esplicito, dalla Commissione europea, tanto all'interno del *Rule of Law Report 2021*¹⁵, quanto dell'*EU Justice Scoreboard 2021*, ove il nostro Paese era stato fatto rientrare tra i sistemi giuridici dell'Unione in cui le «digital solutions to conduct and follow court proceedings in criminal cases» risultavano meno sviluppate¹⁶.

Ed è proprio per far fronte a una tale situazione che con la riforma Cartabia i *conditores* hanno colto l'occasione per introdurre una vasta serie di disposizioni volte a gettare le fondamenta di un vero e proprio “procedimento penale telematico”. Al riguardo, merita subito ricordare come, con tale espressione, si sia soliti indicare un sistema legale che utilizza le tecnologie digitali per gestire elettronicamente le attività e le operazioni che si realizzano «dal momento della redazione della *notitia criminis* fino alla fase definitiva [...] ed

8. INTERNATIONAL MONETARY FUND, *Fostering Growth in Europe Now*, 18 June 2012.

9. EUROPEAN COMMISSION, *EU Justice Scoreboard*, Publications Office of the European Union, 2024.

10. *Amplius*, GALGANI 2022, pp. 5-16.

11. Per questa opinione, v., in dottrina, GALGANI 2022; CANZIO-FIECCONI 2021, p. 147; CURTOTTI-NOCERINO 2024, p. 4; GIALUZ-DELLA TORRE 2022.

12. TONINI 2022, p. 292. Cfr. pure GIALUZ 2022.

13. COUNCIL OF EUROPE, *2022–2025 CEPEJ Action plan: Digitalisation for a better justice*, 9 December 2021.

14. DELLA TORRE 2023, p. 331. Avevamo già proposto un approccio di questo tipo in GIALUZ-DELLA TORRE 2022, p. 7 ss.

15. EUROPEAN COMMISSION, *2021 Rule of law Report*, 20 July 2021.

16. EUROPEAN COMMISSION, The 2021 EU Justice Scoreboard, *COM(2021) 389*, 8 July 2021, p. 36.

all'eventuale esecuzione della pena»¹⁷. Per di più, non va tralasciato il fatto che, nell'ambito di tale macrocategoria, è opportuno distinguere ulteriormente tra il "processo penale telematico in senso stretto" e il "processo a distanza": mentre con la prima locuzione ci si riferisce, più propriamente, ad una gestione online degli atti giudiziari, con la seconda, invece, suole alludersi all'utilizzo della videoconferenza quale strumento che consente l'interazione, in tempo reale, tra persone fisicamente dislocate in luoghi diversi.

Il presente lavoro si colloca nell'ambito di questo complesso quadro di fondo: esso si propone di analizzare pregi, limiti e lacune delle significative novità apportate dalla l. n. 134/2021 e dal d.lgs. n. 150/2022 sul versante della digitalizzazione del procedimento penale. Più in particolare, dopo aver ripercorso il tortuoso cammino che ha caratterizzato il percorso di apertura delle fonti processualpenalistiche interne verso le nuove tecnologie, il cuore del saggio sarà teso ad esaminare alcuni dei principali problemi operativi che la normativa neo-introdotta in materia ha determinato in questo primo periodo di operatività. A tal fine, si cercherà di adottare un approccio il più possibile orientato al dato empirico: è nostra convinzione, infatti, che anche la tematica in esame richieda di essere trattata avendo quale costante punto di riferimento quella che autorevole dottrina ha definito «procedura penale invisibile», cioè quell'insieme di regole e prassi «che non si [possono] leggere nei manuali e nei repertori giurisprudenziali, ma si tocca[no] con mano nella effettività della pratica giudiziaria»¹⁸.

2. Il disorganico quadro normativo previgente

Come si è avuto modo di accennare, il percorso evolutivo che ha portato all'apertura alle nuove tecnologie in ambito processualpenalistico è stato, tradizionalmente, lento e frastagliato, sia per quanto concerne il profilo della smaterializzazione delle udienze, sia in relazione al cd. processo telematico *stricto sensu* inteso.

Dalla prima prospettiva, un primo passaggio chiave si è verificato a seguito dell'introduzione, nel corso degli anni Novanta¹⁹, degli artt. 45-*bis*, 146-*bis* e 147-*bis* disp. att. c.p.p.²⁰, attraverso i quali il legislatore ha aperto all'impiego dei collegamenti a distanza mediante videoconferenza nell'ambito delle reg Giudicande per reati legati alla criminalità organizzata, specie di stampo mafioso.

È risaputo che questo "nucleo" originario di giustizia penale a distanza ha rappresentato «una sorta di breccia di Porta Pia»²¹: da tale momento in poi, infatti, le previsioni in materia sono state via via potenziate nei decenni successivi; e ciò, sia a seguito dell'interpolazione di articoli nuovi²², sia attraverso l'estensione dell'ambito di applicazione di quelli già presenti. A questo proposito spicca, in particolare, quanto fatto dalla cd. riforma Orlando (l. 23 giugno 2017, n. 103), la quale ha dilatato a tal punto il perimetro dell'art. 146-*bis* disp. att. c.p.p.²³, da aver «fatto parlare di una vera e propria "rivoluzione" nella disciplina della partecipazione al dibattimento a distanza, per effetto di una sostanziale "mutazione genetica" di questo meccanismo»²⁴. In buona sostanza, a fronte di una prima fase nella quale la partecipazione da remoto rappresentava una deroga alla presenza fisica nell'aula di udienza, la novella del 2017 aveva, per contro,

17. GALGANI 2019, p. 247. Impiegano, invece, il termine "giustizia elettronica" per descrivere «una vasta gamma di iniziative, tra cui la posta elettronica, la presentazione di ricorsi e la diffusione informatica di informazioni online, il video per audizioni e conferenze, la tracciabilità online della causa, la capacità di accedere alle informazioni per via elettronica», CANZIO-FIECCONI 2021, p. 147 s.

18. Testualmente, AMODIO 2003, p. 1424.

19. Rispettivamente introdotti con la l. 7 gennaio 1998, n. 11 e il d.l. 8 giugno 1992, n. 306.

20. Per un'analisi dei quali, cfr., per tutti, CURTOTTI NAPPI 2006.

21. SIGNORATO 2024, p. 425.

22. Si pensi, ad esempio, all'art. 205-*ter* disp. att., c.p.p. introdotto dalla l. 5 ottobre 2001, n. 367.

23. In proposito, v. l'analisi diacronica di SIGNORATO 2017.

24. Così, testualmente, P. Rivello (2017), p. 139. In merito a tale novella, si vedano, tra i molti, BUZZELLI 2018; DANIELE 2017; MENNA-MINAFRA 2017; LORUSSO 2017; NEGRI 2018.

già trasformato per alcuni soggetti «quella che era un'eccezione in una regola»²⁵, imponendo, di fatto, agli stessi di prendere parte necessariamente a distanza alle attività dibattimentali.

Pur non potendosi soffermare sulla disciplina in parola in questa sede²⁶, merita comunque osservare come questo embrione di “innesto digitale” abbia, fin da subito, provocato un acceso dibattito tra gli studiosi, invero mai del tutto sopito nonostante il *placet* impresso dalla Corte costituzionale e dai giudici europei²⁷. A fronte di censure sollevate con riguardo agli artt. 3, 10, 24, comma 2 e 27, comma 2, Cost., la Consulta ha affermato che «la premessa [sostenuta dal giudice rimettente] secondo cui solo la presenza fisica nel luogo del processo potrebbe assicurare l'effettività del diritto di difesa, non è (...) fondata». Adottando un approccio empirico alla materia, si è, invero, posto in rilievo come l'istituto in parola – e, di conseguenza, ogni forma di *remote participation* – possa dirsi conforme al dettato costituzionale, a condizione, tuttavia, che la strumentazione tecnica impiegata in concreto sia in grado di garantire «un'effettiva partecipazione personale e consapevole dell'imputato al dibattimento»²⁸. Dal che si comprende come la compatibilità dell'istituto con i principi fondamentali del giudizio venga a dipendere, in buona sostanza, dalle concrete modalità di realizzazione del collegamento informatico.

Per quanto concerne, invece, il piano del processo penale telematico “in senso stretto”, i benefici connessi all'impiego della tecnologia hanno indotto il legislatore a intervenire, seppur in modo settoriale, su diversi istituti.

Una prima area di intervento al riguardo, che trova le sue origini sin dagli albori del codice di rito vigente, è, ad esempio, quella che concerne

la dematerializzazione dei registri processuali e, in specie, di quelli relativi alle notizie di reato. Dal punto di vista normativo, l'art. 206 disp. att. c.p.p. stabilisce, infatti, da sempre che con decreto del Ministro della Giustizia vengano adottate le disposizioni regolamentari concernenti «la tenuta, anche in forma automatizzata, dei registri e degli altri strumenti di registrazione in materia penale». In attuazione della predetta prescrizione legislativa, vennero approvati il d.m. 30 settembre 1989, n. 334 e il d.m. 9 novembre 1989 (cd. decreto Vassalli), i quali aprivano le porte a forme di tenuta digitale dei fascicoli, pur non sostituendosi *in toto* quelli cartacei. È, infatti, solo con una successiva interpolazione proveniente da fonti secondarie che si è via via cristallizzata la magmatica disciplina relativa ai registri telematici²⁹, fino a giungere all'adozione del sistema informatizzato SICP (Sistema Informativo della Cognizione Penale), definito come «la chiave di volta nel percorso di informatizzazione dei registri»³⁰. Trattasi, in estrema sintesi, di un modello unico di registro (composto da due sistemi: il cd. Re.Ge Web e il BDMC) o, meglio, di una «banca dati informativa»³¹, nella quale confluiscono tutte le informazioni relative a un determinato procedimento penale. Lo strumento consente, dunque, a tutti i soggetti abilitati di condividere, in uno spazio virtuale, dati giudiziari, nonché di aggiornarli in tempo reale, garantendo maggiore efficacia alle attività decisionali di tutte le componenti coinvolte.

Si collocano quale secondo *step* di questa linea evolutiva le innovazioni apportate nei primi anni Duemila nel settore delle notificazioni. Sfruttando le potenzialità offerte dalle nuove infrastrutture digitali, il legislatore, dopo una prima fase di sperimentazione presso alcuni uffici giudiziari italiani³², ha introdotto, per il tramite dell'art. 4

25. GALGANI 2022, p. 232; NEGRI 2018, p. 569.

26. Cfr., per tutti, CURTOTTI NAPPI 2006; SIGNORATO 2017; TRIGGIANI 2020.

27. Corte Cost., 14 luglio 1999, n. 342; Corte EDU, 5 ottobre 2006, *Viola c. Italia*; Corte EDU, 27 novembre 2007, *Zagaria c. Italia*.

28. Corte cost., 14 luglio 1999, n. 342, par. 3.

29. Si ricordano, in particolare, il d.m. 27 marzo 2000, n. 264 recante il *Regolamento recante norme per la tenuta dei registri presso gli uffici giudiziari* e il d.m. 27 aprile 2009 concernente le *Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia*.

30. GALGANI 2022, p. 145.

31. Così, Cass. pen., Sez. V, 24 settembre 2019, n. 40500, in “OneLegale”.

32. In particolare, il Tribunale e la Procura di Torino.

d.l. 29 dicembre 2009, n. 193³³, in seguito confluito nell'art. 16 d.l. 18 ottobre 2012, n. 179, divenuto efficace il 15 dicembre 2014, un regime di obbligatorietà delle notificazioni telematiche a persone diverse dall'imputato, valevole anche per il procedimento penale³⁴. Anche in questo caso, questo nucleo originario si è con il tempo espanso: con successivi interventi normativi³⁵, il legislatore ha, infatti, man mano ampliato l'ambito di operatività della disciplina, fino a giungere, come si vedrà, con l'approvazione della riforma Cartabia, a una applicazione generalizzata di questa tipologia di notificazione³⁶.

Il modello in origine prescelto (ma tuttora impiegato) si fonda sull'operare congiunto di un'infrastruttura centralizzata *web-based* realizzata dal Ministero della Giustizia, il cd. Sistema Notificazioni Telematiche (SNT), e una serie di caselle di Posta elettronica certificata (PEC) attribuite a ciascun Ufficio giudiziario. L'applicativo così strutturato consente non solamente di inviare notificazioni agli indirizzi inseriti in REGINDE (Registro generale indirizzi elettronici gestito dal Ministero della Giustizia ai sensi del d.m. 21 febbraio 2011, n. 44, che contiene i dati identificativi e l'indirizzo di posta elettronica certificata dei "soggetti abilitati esterni"³⁷), ma anche di monitorare in qualunque momento lo stato del processo d'invio delle medesime, controllando l'avvenuta

ricezione del messaggio anche mediante l'impiego di filtri di ricerca.

Ulteriori passi in avanti verso un processo penale a trazione digitale sono stati, in seguito, realizzati pure con riguardo alla formazione e alla tenuta dei fascicoli. Assume rilievo, al riguardo, la circolare del 26 gennaio 2016 adottata dal DGSIA³⁸ con la quale si è scelto di rendere operativo, dopo una prima fase di sperimentazione, il sistema denominato "Trattamento Informatizzato Atti Penali" (TIAP), ovverosia un software in grado di gestire i fascicoli penali in ogni fase e grado del procedimento³⁹. Trattasi, più in particolare, di un applicativo sviluppato dal Ministero della Giustizia che cura la progressiva formazione dei contenuti delle varie fasi del rito penale, consentendo in tal modo la sua integrazione con atti, documenti e supporti multimediali⁴⁰. Il programma in parola, dunque, lungi dal dover essere assimilato a un mero contenitore di atti e documenti, nasce come strumento per seguire (e registrare) il flusso del processo e dovrebbe, in sostanza, costituire la copia informatizzata del fascicolo processuale cartaceo.

Se un tanto è vero, va peraltro ricordato che, in assenza di una previsione legislativa *ad hoc*, le modalità con le quali procedere alla regolamentazione dell'accesso e della formazione del fascicolo TIAP sono state affidate alla prassi e, più in particolare, alla stipula di appositi protocolli di intesa

33. A mente del quale, «nel processo civile e nel processo penale, tutte le comunicazioni e notificazioni per via telematica si effettuano mediante posta elettronica certificata».

34. Cfr., *amplius*, BOVE 2017; PETRUCCI 2015.

35. Rilevano, in particolare, il d.m. 21 febbraio 2011, n. 44 (*Regolamento Concernente Le Regole Tecniche per l'adozione nel processo civile e nel processo penale, delle tecnologie dell'informazione e della comunicazione*), il d.m. 15 dicembre 2012, n. 209 (*Regole tecniche sulle comunicazioni telematiche*); e il provvedimento del 18 luglio 2011 della Direzione generale per i sistemi informativi automatizzati, *Specifiche tecniche previste dall'art. 34, c.1, del regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal D.lgs 82/2005 e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del Ddl 193/2009, convertito nella legge 24/2010*.

36. Cfr. *infra* par. 6.

37. Cfr. art. 2, comma 1, lett. a), n. 7 del d.m. 29 dicembre 2023, n. 217, il quale include in tale categoria l'avvocatura generale dello Stato, la polizia giudiziaria e ogni alto soggetto tenuto per legge alla trasmissione della notizia di reato e delle comunicazioni successive.

38. Circolare DGSIA 26 gennaio 2016.

39. Per una breve sintesi del funzionamento dello stesso, si veda la Delibera plenaria del CSM del 9 gennaio 2019, *Relazione del CSM sullo stato della giustizia penale telematica 2018*, nonché GIORDANO 2019; GIORDANO 2018.

40. In questi termini, Cass. pen., Sez. V, 7 marzo 2019, n. 27315, in "OneLegale". Cfr. pure MADDALENA 2019.

tra gli uffici giudiziari e le organizzazioni forensi⁴¹. Anche le modalità di visualizzazione e di indicizzazione sono state spesso oggetto del contenuto di accordi para-legali, così come le condizioni di attestazione alle quali l'ufficio fa conseguire la corrispondenza formale tra il fascicolo cartaceo e quello informatizzato al TIAP.

Epperò, nonostante gli evidenti vantaggi legati alla digitalizzazione in questo ambito, deve darsi conto del fatto che, perlomeno fino all'approvazione della riforma Cartabia, il fascicolo telematizzato tramite applicativo TIAP non sostituiva, in alcun caso, il corrispondente cartaceo, giacché il crisma dell'ufficialità era attribuito solo a quest'ultimo⁴². Tanto che la giurisprudenza di legittimità, a fronte del mancato inserimento di un atto di indagine nell'indice del fascicolo digitalizzato tramite TIAP e presente, invece, nell'indice analogico, ha rigettato, a più riprese, le censure di inutilizzabilità sollevate dalla difesa, sottolineando come «le parti non po[tevano] che far fede sul fascicolo processuale cartaceo e di quello devono tenere conto per le loro richieste»⁴³. Il quadro che emergeva era, come giustamente osservato, tutt'altro che rassicurante: l'esercizio di prerogative costituzionalmente garantite – come, ad esempio, l'accesso tempestivo agli atti di indagine, funzionale all'esercizio del diritto di difesa – finiva per dipendere dalla presenza o meno di protocolli e linee guida stabili a livello locale, ovverosia da «contingenze tecniche

e/o territoriali del tutto peculiari [...] condensate in «strani» disposti sub-legislativi»⁴⁴.

Nell'ambito di questo percorso di digitalizzazione di alcuni settori del rito penale, merita di essere ricordata, infine, la creazione del cd. archivio riservato delle intercettazioni, disciplinato agli artt. 269, comma 1, c.p.p. e 89-bis disp. att. c.p.p. Introdotto ad opera del d.lgs. 29 dicembre 2017 n. 216 (cd. riforma Orlando) e successivamente interpolato dalla l. 28 febbraio 2020, n. 7, esso si identifica con i «server che custodiscono, dopo che il pubblico ministero li ha inseriti in esso (cd. conferimento), le registrazioni disposte nell'ambito del procedimento ed i relativi verbali»⁴⁵. L'introduzione di una «cassaforte delle intercettazioni»⁴⁶ rappresenta una novità di non poco rilievo⁴⁷, dal momento che, fino ad allora, il codice del 1988 non aveva previsto alcunché in merito alle modalità (neppure analogiche) di conservazione del materiale rilevante in sede di intercettazione⁴⁸.

L'assenza di una regolamentazione *ad hoc*, specie in una realtà ormai governata dalla bulimica circolazione di dati e informazioni, aveva generato la reazione del Garante italiano per la protezione dei dati personali che, all'esito di un'approfondita istruttoria, rilevava la presenza di «un quadro variegato e disomogeneo di misure, di natura fisica ed informatica, adottate dagli Uffici a protezione delle informazioni personali e dei sistemi [impiegati per la realizzazione delle intercettazioni]»⁴⁹. A fronte di tale quadro, si era, perciò, rivolto un

41. Per alcuni esempi di protocolli, v. GALGANI 2022, p. 164, nt. 138.

42. Cass. pen., Sez. I, 29 aprile 2016, n. 44424, in «OneLegale».

43. Cass. pen., Sez. V, 7 marzo 2019, n. 27315, cit. Conf. Cass. pen., Sez. III, 25 giugno 2018, n. 53986, in «OneLegale».

44. Così, GALGANI 2022, p. 166. Egualmente critica è BOVE 2015.

45. SIGNORATO 2017, p. 82. Dal punto di vista normativo, v. la definizione contenuta nel *Provvedimento 23 dicembre 2020 - Provvedimento del Direttore generale dei servizi informativi automatizzati di modifica e sostituzione delle specifiche tecniche per il conferimento nell'archivio digitale delle intercettazioni di cui all'art. 269 comma 1 c.p.p.*, 23 dicembre 2020, ove ci si riferisce a un «sistema informatico (*hardware* e *software*) che consente di conservare tutte le conversazioni e comunicazioni disposte nell'ambito del procedimento, nonché di classificarle, in conformità alla relativa disciplina procedimentale; il sistema rende altresì disponibili le funzioni di accesso e di ascolto delle conversazioni o comunicazioni registrate».

46. Così, FILIPPI 2018, p. 37.

47. Tanto che CAMON 2018, p. 79 la definisce come «il fiore all'occhiello della riforma».

48. L'art. 269 c.p.p. stabiliva semplicemente che i verbali e le registrazioni delle intercettazioni venissero «conservati integralmente presso il pubblico ministero che [aveva] disposto l'intercettazione».

49. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento in materia di misure di sicurezza nelle attività di intercettazione da parte delle Procure della Repubblica*, 18 luglio 2013, n. 356.

invito al legislatore affinché adottasse misure idonee ad assicurare una tendenziale omogeneità delle discipline volte alla tutela dei dati personali dei soggetti coinvolti (indagati e, specialmente, terzi estranei alle indagini). A ben riflettere, perciò, la scelta a favore di un “archivio digitale”, ove allocare le registrazioni e i verbali risultanti dalle attività di captazione, non è stata dovuta tanto ad una (pur auspicata) attività di riorganizzazione logistica degli uffici giudiziari di Procura, bensì alla necessità di adottare misure e accorgimenti volti a rafforzare il controllo preventivo e la sicurezza nel trattamento dei dati personali nell’ambito dell’attività di intercettazione.

Giunti a questo punto, è il caso di ricordare come il frastagliato quadro evolutivo finora ricostruito abbia subito una significativa accelerazione a seguito dello scoppio della pandemia da Covid-19⁵⁰. L’impossibilità di mantenere contatti sociali *de visu* ha, infatti, portato anche il legislatore italiano ad adottare una vasta serie di disposizioni emergenziali, caratterizzate da scadenze connesse all’andamento del contagio, volte a consentire di far leva sugli strumenti informatici, onde garantire comunque la prosecuzione in sicurezza del servizio giustizia⁵¹. Nell’economia del presente lavoro, due sono le innovazioni principali, introdotte in questo contesto, che meritano di essere ricordate.

Per un verso, il legislatore ha sviluppato il “Portale Deposito Atti Penali” (PDP), ovvero sia

una piattaforma internet che consentiva (e consente tuttora) ai difensori, con riguardo a una specifica categoria di atti (successivi alla notifica dell’avviso *ex art. 415-bis c.p.p.*), di eseguire il deposito digitale su un sistema informatico messo a disposizione dal Ministero della Giustizia.

Per altro verso, si è optato per una maggiore apertura al processo penale a distanza⁵². Al riguardo, è sufficiente menzionare come il legislatore italiano, con il d.l. 2 marzo 2020, n. 19, passando per il decreto cd. “cura Italia”⁵³ ed il cd. decreto “ristori”⁵⁴ sino ad approdare al d.l. 23 luglio 2021, n. 1059, abbia introdotto una legislazione che autorizzava l’autorità giudiziaria a fare ampio uso dello strumento dell’udienza “da remoto”⁵⁵, pur con tutta una serie di limitazioni di carattere soggettivo e oggettivo⁵⁶.

Ciò che importa, ai nostri fini, è mettere in rilievo come la disciplina pandemica, nonostante le inevitabili criticità derivanti dalla necessità di elaborarla in tempi rapidissimi, abbia consentito di sperimentare forme del tutto innovative di gestione informatizzata delle procedure giudiziarie⁵⁷. Essa, più in particolare, ha rappresentato un «laboratorio giuridico»⁵⁸ che è servito quale essenziale punto di riferimento per lo sviluppo di quello che, da lì a breve, è divenuto il nuovo “processo penale telematico Cartabia-style”.

50. Come rileva giustamente TRAPPELLA 2022, p. 1008 «senza la pandemia, la digitalizzazione del procedimento penale sarebbe rimasta ai margini degli interessi del normatore». Anche secondo GIORDANO 2021 la «spinta all’impiego dell’informatica nel processo penale è stata determinata dall’avvento della pandemia».

51. Sia consentito il rinvio a DELLA TORRE 2023, p. 253.

52. Sul punto la letteratura è molto ampia: si vedano, anche per ulteriori riferimenti bibliografici, AMODIO-CATALANO 2020; GIORDANO 2020-B; LORUSSO 2020; MANCUSO 2020; MAZZA 2020; NAPOLITANO 2020; RUGGIERI 2020.

53. D.l. 17 marzo 2020, n. 18, convertito con modificazioni dalla l. 24 aprile 2020, n. 27.

54. D.l. 28 ottobre 2020, n. 137, convertito con modificazioni dalla l. 18 dicembre 2020, n. 176.

55. Sull’indebito utilizzo dell’espressione “da remoto” in relazione all’udienza telematica, v. AMODIO 2020.

56. Si veda, più in dettaglio, NAPOLITANO 2020.

57. Invero, mette conto ricordare come, ancor prima dell’insorgere della pandemia, il disegno di legge C. 24351 (cd. ddl Bonafede) avesse gettato le basi normative per una più massiccia informatizzazione del processo penale. Le novità, a tal proposito, riguardavano, da un lato, la proposta di generalizzare l’utilizzo della PEC per compiere comunicazioni o notificazioni a persona diversa dall’imputato e, da un altro lato, la possibilità di provvedere al deposito di atti e documenti con modalità tecnologiche accelerate. Cfr., *amplius*, GIALUZ-DELLA TORRE 2020; GIORDANO 2020-A.

58. CAIANIELLO-PUGLIESE 2024, p. 180.

3. Le novità apportate dalla riforma Cartabia

Come si è anticipato, la riforma Cartabia ha determinato un ulteriore cambio di passo nella materia in esame. Facendo tesoro delle potenzialità emerse dalle “sperimentazioni” digitali in epoca Covid, il legislatore, essendo chiamato ad adottare una novella capace di rilanciare l’efficienza dell’ordinamento penale nel suo complesso, ha pensato di introdurre finalmente una disciplina generale e organica del processo penale telematico nelle sue varie componenti.

Sotto un primo profilo, l’obiettivo perseguito dai *conditores* è stato quello di creare, sulla scorta di quanto già implementato in sede civile, una sorta di “cancelleria telematica”⁵⁹, espressione con la quale alludiamo a tutte quelle attività che consentono non solo il caricamento e la consultazione elettronica (e da remoto) degli atti giudiziari, ma anche la gestione online delle operazioni realizzate nel corso del procedimento (consultazione del calendario dei processi, utilizzo dei sistemi di pagamento virtuali per le spese processuali, etc.). Si inseriscono in tale contesto, ad esempio, le modifiche apportate alla disciplina concernente la natura e la verbalizzazione degli atti, la tenuta dei fascicoli, le notificazioni e i depositi.

Sotto un secondo profilo, si è voluto implementare e, allo stesso tempo, conferire organicità all’istituto della partecipazione a distanza, che, come si è accennato, ha rappresentato uno strumento a cui è stato attribuito grande rilievo nel corso del periodo pandemico.

Nel prosieguo della trattazione verranno analizzate entrambe tali aree di intervento, mettendosi in luce i loro punti di forza, nonché i difetti e le lacune che le caratterizzano.

4. I pilastri del nuovo processo penale 2.0: l’atto nativo digitale, il fascicolo informatico e le novità in tema di verbalizzazione

Il primo dato su cui va concentrata l’attenzione è la circostanza per cui il nuovo procedimento penale *paperless*, costruito dal d.lgs. n. 150/2022, si fonda su due pilastri normativi fondamentali.

Il primo è costituito dall’art. 110 c.p.p., il quale stabilisce, in modo del tutto innovativo, che gli atti processuali devono, di norma, essere creati e conservati esclusivamente in forma digitale, garantendone l’autenticità, l’integrità, la leggibilità, l’interoperabilità e, ove richiesto dalla legge, la segretezza. Come era inevitabile, nel fornire una «nuova identità all’atto processuale»⁶⁰, il legislatore ha avuto cura di mantenere, in via di eccezione, un “regime analogico” per tutti quegli atti che, per loro «natura o per specifiche esigenze processuali», non possono essere redatti in forma di «documento informatico»⁶¹.

Benché la norma appaia tutto sommato chiara e intelleggibile, deve, tuttavia, darsi conto di un contrasto sviluppatosi con riguardo alla compatibilità della nuova regolamentazione con il canone di legalità processuale. Oggetto di dibattito è, in particolare, il contenuto del secondo comma, nella parte in cui rinvia ad altra «normativa, anche regolamentare» per una più precisa individuazione della disciplina in tema di redazione, sottoscrizione, conservazione, accesso, trasmissione e ricezione degli atti e dei documenti. Ebbene, parte degli studiosi ha censurato tale meccanismo, giacché, «lungi dall’essere un mero riempitivo di cognizioni tecnico-informatiche, il richiamo ai regolamenti – e, vista la confusione classificatoria tra i riferimenti nell’ambito, alla *soft-law* – è capace di incidere sull’ampiezza delle garanzie costituzionali»⁶². A ben pensare, però, la scelta appare giustificata dal cd. principio di neutralità tecnologica; principio che permea l’intera legislazione

59. Parlano di una «informatizzazione dei servizi di cancelleria» quale obiettivo primario della riforma Cartabia sul versante del processo penale telematico, CAIANIELLO–PUGLIESE 2024, p. 180.

60. GALGANI 2023-A, p. 404.

61. Sull’inappropriatezza dell’utilizzo di tale terminologia, v. GALGANI 2023-A, pp. 407-409.

62. TRAPPELLA 2022, p. 1009. Di «comprensibili timori circa il rispetto della fondamentale riserva di legge» ha parlato TRABACE 2023, p. 26.

di nuovo conio⁶³. Con tale espressione si allude al fatto che la normativa di fonte primaria dovrebbe astenersi dall'individuare specifiche soluzioni tecniche per la realizzazione delle attività processuali, dal momento che l'evoluzione tecnologica rischia di rendere obsolescenti e inadeguate le nuove disposizioni ancor prima della loro entrata in vigore. In questa prospettiva, e al pari di quanto suggerito in altri ambiti⁶⁴, sembra, dunque, ragionevole la semplice previsione, a livello codicistico, di principi generali e astratti, ai quali poi il "legislatore tecnico" dovrà dare attuazione, pur sempre nel rispetto delle linee guida fissate a livello astratto e generale⁶⁵.

Una volta attribuita natura digitale all'atto processuale, i *conditores* si sono, coerentemente, premurati di superare il tradizionale sistema di catalogazione e conservazione imperniato sui cd. "faldoni", istituendo l'obbligatorietà della tenuta informatica dei fascicoli. E in questa prospettiva è stato introdotto, quale secondo pilastro del nuovo sistema, l'art. 111-ter c.p.p., il quale stabilisce che detti "raccoltori 2.0" siano formati, conservati e aggiornati digitalmente, in modo da garantirne l'autenticità, l'integrità, l'accessibilità, la leggibilità,

l'interoperabilità e la facile consultazione online da parte di tutti i soggetti autorizzati.

Pure tale novità – benché debbano essere a tutt'oggi risolte alcune questioni tecniche legate al concreto funzionamento dei sistemi informatici di gestione⁶⁶, ma ricche di implicazioni sul piano giuridico⁶⁷ – merita di essere accolta con favore. Numerosi, sono, infatti, i benefici che potranno derivare da una gestione interamente digitalizzata dei fascicoli, specie con riguardo alla riduzione dei cd. tempi morti del loro attraversamento, che, come noto, rappresentano una delle cause più critiche di irragionevole durata dei nostri procedimenti, specie con riguardo al passaggio dal primo grado all'appello⁶⁸. Da questo punto di vista, il legislatore pare, in definitiva, aver ben fatto proprio lo spirito delle indicazioni provenienti dal già richiamato 2022-2025 *Action plan*⁶⁹, nel quale la CEPEJ ha sottolineato proprio la necessità per gli Stati membri di realizzare, quanto prima, una completa «transition from paper to digital court files» nell'ottica di garantire una maggiore "efficienza qualitativa" dell'apparato giudiziario.

In detto scenario, peraltro, deve darsi altresì conto di una novità di estremo rilievo concernente

63. Così, CAIANIELLO-PUGLIESE 2024, p. 189. Non intravede una violazione della legalità processuale neppure GALGANI 2023-A, p. 420 s.

64. Il riferimento è, in particolare, ai mezzi di ricerca della prova tecnologici: cfr. CAIANIELLO 2022, p. 243; LASAGNI 2016. Parimenti, è stato osservato, sotto il profilo delle *best practices* forensi impiegate nel contesto della *digital evidence*, che l'individuazione a livello legislativo di una singola tecnica di acquisizione si pone in contrasto con l'idea di una scienza informatica "in continua evoluzione", non potendosi individuare, allo stato dell'arte, una modalità apprensiva in grado di imporsi sulle altre. Senza voler considerare, in aggiunta, come la scelta di una metodologia piuttosto che l'altra dipenda, nella maggior parte dei casi, dalle circostanze del caso concreto: DANIELE 2011, p. 293.

65. Concorde GALGANI 2023-A, p. 406 s.

66. Ciò vale, ad esempio, per l'applicativo APP (cfr. *infra* par. 5).

67. GALGANI 2023-A, p. 423, la quale ricorda, ad esempio, il tema relativo alla *data entry* e cioè «se l'inserimento dei materiali [nel fascicolo digitale] dovrà essere sempre e comunque mediato dall'intervento del personale di segreteria e di cancelleria [...] o, per contro, potrà valere il deposito "diretto" da parte degli utenti». Al riguardo, l'art. 19, punto n. 9 delle *Specifiche tecniche* adottate dal Direttore generale per i sistemi informativi automatizzati in data 2 agosto 2024 (ed entrate in vigore il 30 settembre 2024) prevede che «a seguito dell'invio dell'atto processuale i sistemi informativi ministeriali procedono alla verifica ed accettazione automatica del deposito degli atti inviati dai difensori rispetto ai quali vi è corrispondenza tra i dati inseriti sul PDP ed i dati di registro del procedimento penale, senza intervento degli operatori di segreteria e di cancelleria». Cfr. anche CAIANIELLO-PUGLIESE 2024, p. 201.

68. DELLA TORRE 2022, p. 49; GIALUZ 2022, p. 10.

69. CEPEJ, *2022-2025 Action Plan*, 9 December 2021.

il tema della verbalizzazione degli atti⁷⁰. In sintonia con il principio enunciato dall'art. 1, comma 8, lett. a) e b), della legge delega, il d.lgs. n. 150/2022 ha modificato il contenuto dell'art. 134 c.p.p. stabilendo che la riproduzione audiovisiva o fonografica deve ritenersi la modalità ordinaria di documentazione delle attività procedurali. Il regime di *favor* manifestato, in questo contesto, per l'impiego di strumentazioni digitali «risponde all'esigenza di rendere più completa e, quindi, più fedele la verbalizzazione»⁷¹, assicurando in tal modo una rappresentazione più accurata dell'atto realizzato. L'obiettivo che si intende perseguire è, all'evidenza, duplice. Per un verso, l'impiego della tecnologia consente di realizzare un controllo *ex post* sul rispetto dei diritti fondamentali dei soggetti coinvolti nell'atto, specie – ma non esclusivamente⁷² – con riguardo a quelli compiuti dagli organi di indagine nella fase previa⁷³. Per altro verso, sulla scorta delle indicazioni provenienti dalla giurisprudenza di Strasburgo⁷⁴, dalle fonti eurounitarie⁷⁵ e dalla stessa Corte costituzionale⁷⁶, l'introduzione di siffatto meccanismo funge da rimedio compensativo rispetto alle deroghe al principio di immediatezza. Ai sensi del nuovo art. 495, comma 4-ter c.p.p., infatti, la documentazione integralmente audiovisiva dell'assunzione di fonti orali osta alla rinnovazione del dibattimento in caso di mutamento del giudice, salvo che quest'ultimo non la ritenga comunque necessaria sulla base di specifiche esigenze⁷⁷.

4.1. Il deposito telematico

In ottemperanza al *dictum* contenuto nell'art. 1, comma 5, lett. a), l. n. 134/2021, il legislatore ha introdotto, quale ulteriore elemento cardine del sistema di procedimento penale *paperless*, un nuovo art. 111-*bis* c.p.p., ove si stabilisce che gli atti processuali, salvo il caso di malfunzionamenti dei sistemi informatici dei domini del Ministero della Giustizia (art. 175-*bis* c.p.p.)⁷⁸, devono essere depositati, in tutte le fasi del rito, in modalità esclusivamente telematica.

Al riguardo, va posto subito in rilievo come siffatte disposizioni siano portatrici di «un vero e proprio cambio di paradigma»⁷⁹, specie se raffrontate al previgente sistema nel quale i draconiani orientamenti della giurisprudenza di legittimità avevano alquanto limitato l'impiego di strumentazioni elettroniche (e, in particolare, della PEC) per il deposito degli atti processuali⁸⁰. Proprio onde superare le resistenze tradizionali che avevano interessato in particolare gli atti di impugnazione, il legislatore ha scelto di chiarire, in modo esplicito, all'art. 582, comma 1, c.p.p. che anche i gravami vanno oggi presentati, di norma, mediante deposito con le modalità previste dall'articolo 111-*bis* c.p.p. nella cancelleria del giudice che ha emesso il provvedimento impugnato.

Ciò premesso, va ricordato che i *conditores* hanno individuato tre eccezioni alla regola generale che impone la digitalizzazione delle modalità di deposito.

70. BONZANO 2022; DUCOLI 2023; LOPEZ 2022.

71. CIAVOLA 2023, p. 68.

72. Art. 510, comma 2-*bis*, c.p.p.

73. Si vedano, ad esempio, gli artt. 141-*bis*, 351, 362 c.p.p.

74. Corte EDU, 23 maggio 2019, *Doyle c. Irlanda*, par. 99; Corte EDU, 15 dicembre 2015, *Schatschaschwili c. Germania*, par. 127.

75. Cfr., ad esempio, il considerando 53 e l'art. 24 della direttiva 2012/29/UE.

76. Corte cost., 29 maggio 2019, n. 132.

77. L'art. 93-*bis* del d.lgs. n. 150/2022, modificato dal d.l. n. 162/2022 ha previsto che la disposizione di cui all'art. 495, comma 4-ter c.p.p. «non si applica quando è chiesta la rinnovazione dell'esame di una persona che ha reso le precedenti dichiarazioni in data anteriore al 1° gennaio 2023».

78. Cfr. *infra* par. 5.

79. CAIANIELLO-PUGLIESE 2024, p. 191. Cfr. pure GALGANI 2023-B, p. 114. Di «una disposizione cardine nell'impalcatura del processo penale telematico» ha parlato GIALUZ 2022, p. 6.

80. Cfr., ad esempio, Cass. pen., Sez. VI, 27 novembre 2019, n. 52092, in *OneLegale*; Cass. pen., Sez. III, 13 aprile 2018, n. 38411, *ivi*; Cass. pen., Sez. VI, 5 dicembre 2017, n. 271677, *ivi*. Per un quadro di sintesi, v. GIORDANO 2021; GALGANI 2022, p. 167 ss.; LA ROCCA 2019.

Anzitutto, è consentito procedere in forma analogica con riguardo ad atti e documenti che non possono essere acquisiti in copia informatica in ragione: a) della loro natura; b) di specifiche esigenze processuali. Se con riguardo alla prima ipotesi non sembrano profilarsi problemi di particolare rilievo⁸¹, più complessa appare l'opera volta a circoscrivere l'ambito applicativo del parametro *sub b)*. Potrebbero assumere una certa consistenza, in proposito, tutte le circostanze in cui un determinato atto può essere presentato direttamente in udienza, come una dichiarazione di costituzione di parte civile o l'esibizione di un documento in sede di *cross-examination*⁸².

Ulteriore ipotesi eccezionale è quella sancita all'ultimo comma dell'art. 111-*bis*, a mente del quale gli atti che le parti e la persona offesa dal reato compiono personalmente possono essere depositati anche con modalità non telematiche. Invero, la versione originaria del testo non operava alcun riferimento alla vittima, ma, al riguardo, il d.lgs. 19 marzo 2024, n. 31⁸³, recependo i suggerimenti provenienti da una parte della dottrina⁸⁴, ha opportunamente esteso siffatto meccanismo.

Nell'ottica di favorire l'esercizio del diritto di difesa⁸⁵ e sfruttare appieno le potenzialità del "formante tecnologico", il legislatore è intervenuto pure sull'art. 172 c.p.p., stabilendo che il termine per fare dichiarazioni, depositare documenti o compiere altri atti in un ufficio giudiziario con modalità telematiche si considera rispettato se l'accettazione dello stesso da parte del sistema informatico avviene entro le ore 24 dell'ultimo giorno utile. Si è altresì precisato che i termini decorrenti

dal deposito telematico degli atti effettuato fuori dell'orario d'ufficio stabilito dal regolamento si computano dalla data della prima apertura immediatamente successiva.

Infine, la consapevolezza circa le disfunzioni tecniche che possono riguardare (e che, nella prassi quotidiana, riguardano) gli applicativi tecnologici in uso presso gli uffici giudiziari, ha portato il legislatore del 2021 a delegare l'esecutivo ad adottare una disciplina rimediabile *ad hoc*, al fine di evitare che eventuali malfunzionamenti potessero pregiudicare l'esercizio delle facoltà difensive. In attuazione di tale direttiva, il governo ha regolato la materia nel nuovo art. 175-*bis* c.p.p., ove vengono oggi disciplinate due distinte ipotesi (nonché le relative conseguenze processuali) di malfunzionamento dei sistemi informatici.

La prima concerne il caso in cui i *bug* di sistema emergano con riguardo ai domini informatici del Ministero della Giustizia, mentre la seconda è relativa ai malfunzionamenti che possono verificarsi in uno specifico ufficio giudiziario locale. Nella prima evenienza, il malfunzionamento, per assumere rilevanza in termini giuridici, deve essere certificato dal Direttore generale dei Servizi Informatici Automatizzati del Ministero della Giustizia e successivamente comunicato in modo da garantirne la conoscenza al pubblico (avvocati, *in primis*). Nella seconda, invece, l'art. 175-*bis* c.p.p. stabilisce che sia il capo dell'ufficio a verificare il malfunzionamento e, anche in questo caso, a comunicarlo con mezzi in grado di assicurarne la tempestiva conoscenza. In entrambe le situazioni è previsto che, durante il periodo di stallo, gli atti e

81. La *Relazione illustrativa al d.lgs. n. 150/2022*, p. 191 s. cita, in proposito, i «documenti aventi contenuto dichiarativo preformati rispetto al processo penale (una scrittura privata, un testamento olografo) di cui si contesti l'autenticità o documenti, quali ad esempio planimetrie, estratti di mappa, fotografie aeree satellitari, per i quali appare indispensabile il deposito in forma di documento analogico, posto che l'acquisizione in forma di documento informatico priverebbe di nitidezza e precisione i relativi dati, incidendo sul loro valore dimostrativo in sede processuale».

82. Sulla stessa linea di pensiero, v. CAIANIELLO-PUGLIESE 2024, p. 194.

83. Cfr. GIALUZ 2024.

84. GALGANI 2023-A, p. 413; GIALUZ 2022, p. 7, per il quale «il rischio sarebbe stato quello di pregiudicare l'effettività dell'accesso alla giustizia e del diritto di difesa di quei soggetti, tra cui, soprattutto, l'imputato, privi di conoscenze tecnologiche»; PORCU 2022, p. 72.

85. Come esplicitato nella *Relazione illustrativa al d.lgs. n. 150/2022*, cit., p. 19 il *novum* ha inteso rafforzare «l'esercizio del diritto di difesa, in quanto la parte può far uso dell'intera giornata nella quale è in scadenza il lasso temporale previsto dalla legge per depositare telematicamente l'atto».

i documenti debbano essere prodotti e depositati in “formato analogico”.

L'ultimo comma della disposizione è dedicato al caso in cui la scadenza di un termine perentorio previsto a pena di decadenza intervenga nel corso del periodo di malfunzionamento. Si introduce, al riguardo, una speciale ipotesi di restituzione nel termine *ex art. 175 c.p.p.*, prevedendo opportunamente che le parti possano esercitare i diritti e le facoltà loro spettanti qualora provino di essersi trovate, per caso fortuito o forza maggiore, nell'impossibilità di redigere o depositare tempestivamente l'atto in forma cartacea.

Come si vedrà meglio a seguire⁸⁶, la nuova disciplina di carattere rimediale, a fronte di un'inadeguatezza delle apparecchiature tecniche, è già stata applicata, nella prassi, con una certa disinvoltura, essendo oggetto di interpretazioni estensive volte a sospendere *sine die* l'utilizzo dei sistemi informatici per la realizzazione dei depositi.

4.1.1. Verso una nuova tipologia di invalidità processuale? L'“atto abilitante” e il concetto di “irricevibilità”

Detto ciò, va rilevato che l'argomento del deposito telematico non presenta solo luci, ma anche significative ombre. Tra queste spicca il profilo del cosiddetto “atto abilitante”.

L'istituto in parola è stato introdotto dall'art. 5, comma 1, n. 4) del Provvedimento del Direttore del DGSIA del 24 febbraio 2021 per esigenze legate al funzionamento del Portale Deposito Atti Penali e al fine di tutelare il segreto investigativo, scongiurando la pratica di nomine puramente esplorative⁸⁷. Più nello specifico, la locuzione in esame si riferisce a quell'«atto da cui risulti la conoscenza dell'esistenza di un procedimento relativo al proprio assistito e il relativo numero di Registro»⁸⁸. In

pratica, al fine di poter depositare la nomina del difensore di fiducia (ed eventuali atti successivi), il Portale richiede un titolo abilitante, ossia un documento che dimostri la conoscenza del procedimento e del numero progressivo indicato nel registro delle notizie di reato. La disciplina in parola, come stabilito nel provvedimento del DGSIA, è destinata a trovare applicazione nella sola fase delle indagini preliminari, ovverosia qualora non sia ancora stato emesso uno degli avvisi *ex artt. 408, 411 o 415-bis c.p.p.*, risultando, dunque, illegittimo, ogni rifiuto riferito a depositi di nomine successive all'avvenuta *discovery*⁸⁹.

Nonostante il regime cronologico da ultimo segnalato, non è difficile rendersi conto di come il meccanismo in esame rischi di ostruire in modo sproporzionato l'esercizio di vari diritti costituzionalmente garantiti, tra cui *in primis* quello di difesa⁹⁰, perlomeno tutte le volte in cui l'indagato e il suo difensore siano a conoscenza della pendenza del procedimento, ma non anche del corrispettivo numero di iscrizione.

È ben vero – si obietterà – che tale informazione potrebbe essere acquisita attraverso la proposizione di una richiesta formulata ai sensi dell'art. 335, comma 3, c.p.p. Ed è altrettanto vero che, a differenza di quanto previsto in passato, l'istanza volta a ottenere detta certificazione può essere oggi presentata direttamente tramite il Portale. Cionondimeno, vi possono essere casi, tutt'altro che infrequenti nella prassi, nei quali un tale adempimento risulti incompatibile con le tempistiche imposte per l'esercizio dei diritti difensivi: si pensi, ad esempio, a un procedimento cautelare, laddove l'assistito, per qualsiasi ragione, non sia in possesso della copia del provvedimento.

In tale situazione, la necessità di proporre un gravame in tempi brevi è radicalmente incompatibile con una richiesta *ex art. 335, comma 3,*

86. Cfr. *infra* par. 5.

87. *Provvedimento del Direttore del DGSIA* del 24 febbraio 2021.

88. *Ibidem*.

89. *Ibidem*.

90. Critiche all'introduzione dell'atto abilitante sono state avanzate da GALGANI 2022, p. 178; TAVASSI 2024, pp. 19-20; TRAPELLA 2022, p. 1012 il quale soggiunge come si tratti di «un adempimento contrario ai precetti minimi dei rapporti con la pubblica amministrazione, atteso che si tratta di inviare all'apparato copia di un atto di cui è già in possesso perché, semplicemente, ne è l'autore».

c.p.p.⁹¹; richiesta che gli uffici, come dimostra la prassi quotidiana, non sono talvolta in grado di evadere in tempi celeri. Per non dire poi delle fattispecie in cui, stando alla disciplina dell'art. 110-bis disp. att. c.p.p., la Procura può rispondere a un'istanza di questo tipo con la sibillina formula «non risultano iscrizioni suscettibili di comunicazione».

Al netto delle problematiche appena segnalate, non si può fare a meno di notare come la procedura concernente il deposito dell'atto abilitante sembri aver surrettiziamente introdotto, nel nostro modello processuale, una nuova forma di invalidità extra-legale (e, in quanto tale, contrastante con i principi di base della materia della legalità processuale e della tassatività), destinata ad operare esclusivamente in *malam partem*: ovvero sia la «irricevibilità». L'omesso caricamento nel Portale dell'atto abilitante, infatti, comporta automaticamente la non accettazione dell'atto derivato (cioè, la nomina del difensore), inibendone pertanto l'efficacia processuale e impedendo l'instaurazione di un confronto tra accusa e difesa nella fase delle indagini preliminari. Per di più, la genericità del concetto di «atto abilitante», rispetto al quale non viene operata alcuna specificazione nei vari provvedimenti del DGSIA, finisce per legittimare prassi distorte volte a includervi, per ragioni non meglio specificate, solamente alcune tipologie di atti processuali, in specie il provvedimento da cui risulta l'iscrizione *ex art.* 335 c.p.p.⁹².

4.1.2. Il d.m. 29 dicembre 2023, n. 217 e la disciplina intertemporale e transitoria per i depositi

Come era prevedibile, la svolta tecnologica determinata dal d.lgs. n. 150/2022 ha suscitato forti preoccupazioni di ordine pratico, tanto nella classe forense quanto nella magistratura, circa i problemi che sarebbero derivati da una sua completa immediata applicazione nell'arretrata realtà italiana. Al riguardo, si è, infatti, a più voci messo giustamente in luce come, in mancanza di adeguate opere di potenziamento, l'infrastruttura in uso nella maggior parte delle sedi giudiziarie fosse del tutto inadeguata, nonché quantitativamente e qualitativamente insufficiente, per consentire una gestione digitale generalizzata dei documenti e degli atti processuali⁹³.

È in tale contesto problematico che si colloca la stratificata disciplina di matrice intertemporale e transitoria ideata sul punto dal riformatore, che trova la sua sede normativa principale nell'art. 87 del d.lgs. n. 150/2022⁹⁴, il quale ha trovato attuazione tramite il d.m. 29 dicembre 2023, n. 217⁹⁵; fonte che, oltre a dettare regole tecniche riguardanti il deposito, la comunicazione e la notificazione con modalità telematiche degli atti processuali, ha rinviato l'entrata in vigore di molte disposizioni cardine in materia di processo penale telematico al 31 dicembre 2024⁹⁶.

Se ciò è vero, va rilevato come il decreto in questione, facendo propria una logica dei «piccoli passi», non abbia rinunciato comunque a sperimentare

91. Per di più, si osservi come i malfunzionamenti del sistema informatico possano non di rado inibire il corretto deposito dell'atto abilitante: si veda, ad es., il caso *paradigmatico* nel quale l'istanza avanzata *ex art.* 415-bis c.p.p. è stata rifiutata perché, nel testo della medesima, vi era un errore nell'indicazione di una lettera del cognome dell'indagato.

92. Se ne dà conto in UCPI, *Brevi considerazioni sulle specifiche tecniche per i depositi degli atti*, 9 agosto 2024.

93. UCPI, *Processo telematico: soddisfazione per la proroga dell'attuale regime di deposito*, 31 dicembre 2023; PALMIERI 2023.

94. Ai sensi del primo comma dell'art. 87, il Ministro della giustizia, con decreto da adottarsi entro il 31 dicembre 2023, sentito il Garante per la protezione dei dati personali, avrebbe dovuto definire le regole tecniche riguardanti il deposito, la comunicazione e la notificazione con modalità telematiche degli atti del procedimento penale, anche modificando, ove necessario, il regolamento di cui al decreto del Ministro della giustizia 21 febbraio 2011, n. 44, e, in ogni caso, assicurando la conformità al principio di idoneità del mezzo e a quello della certezza del compimento dell'atto.

95. D.m. 29 dicembre 2023, n. 217, sul quale v. CURTOTTI-NOCERINO 2024.

96. Occorre precisare, al riguardo, che le nuove norme in tema di notificazioni sono entrate formalmente in vigore già dal 30 dicembre 2022 (art. 6 d.l. n. 162/2022).

l'immediata applicazione del nuovo regime per quanto concerne alcune fasi del rito. A questo proposito, l'art. 3, comma 1, stabilisce, in particolare, che, di regola, il deposito di atti, documenti, richieste e memorie nel corso della fase delle indagini preliminari abbia da subito luogo esclusivamente con modalità telematiche ai sensi dell'art. 111-*bis* c.p.p., presso la procura della Repubblica, la procura europea, l'ufficio g.i.p. e la procura generale presso la corte di appello, limitatamente al procedimento di avocazione. In via di eccezione, però, il comma 7 della medesima disposizione, nel prevedere un regime transitorio valido sino al 31 dicembre 2024, statuisce che il deposito da parte dei "soggetti abilitati interni"⁹⁷ di atti, documenti, richieste e memorie possa avvenire anche con «modalità non telematiche», ovvero, in ragione del principio di equivalenza contenuto al comma 8⁹⁸, mediante l'impiego della PEC. La deroga, tuttavia, non trova applicazione per gli atti relativi ai procedimenti di archiviazione e alla riapertura delle indagini, per i quali torna nuovamente ad applicarsi la regola del deposito obbligatorio di tipo telematico.

Per quanto concerne i difensori, l'art. 3, comma 2, individua, quale principio generale, quello del deposito a mezzo Portale di atti, documenti, richieste e memorie, presso la corte di appello, il tribunale ordinario, il giudice di pace, la procura generale presso la corte di appello, la procura della Repubblica presso il tribunale e la Procura europea. Anche in questo caso, però, il decreto introduce un regime transitorio valido sino al 31 dicembre 2024. Ai sensi dell'art. 3, comma 8, gli avvocati possono sempre realizzare depositi con «modalità non telematiche», ad esclusione di quelli relativi alla fase delle indagini preliminari, al procedimento di archiviazione e alla riapertura delle indagini, nonché della nomina, della rinuncia o revoca del mandato, per i quali torna in vigore l'ordinario regime di trasmissione a mezzo Portale. Tale ultima preclusione, tuttavia, non opera («eccezione all'eccezione») con riguardo al deposito di atti e

documenti nei procedimenti relativi all'impugnazione dei provvedimenti in materia di cautelare o in materia di sequestro probatorio emessi durante la fase delle indagini preliminari.

La disciplina della quale si è dato conto, pur apprezzabile nell'intento di voler dare concreta attuazione ai principi contenuti nel d.lgs. n. 150/2022, lascia molto a desiderare, specie con riguardo alla tecnica legislativa impiegata. In effetti, l'articolato normativo, imperniato su un alternarsi di regole ed eccezioni, appare davvero poco chiaro e affatto intelleggibile.

5. Il nuovo applicativo ministeriale per la gestione del fascicolo telematico: cd. APP

Così ricostruita la disciplina a livello legislativo, va segnalato come, in sede di attuazione, il Ministero della Giustizia, con l'obiettivo di ottimizzare la gestione degli atti e dei documenti processuali – secondo parametri di semplicità, celerità, trasparenza e fruibilità – abbia creato un nuovo sistema cui è affidata la concreta realizzazione del processo telematico. Il riferimento corre al cd. Applicativo del Processo Penale (APP) che, dopo una brevissima fase di sperimentazione presso alcuni uffici di Procura iniziata nel mese di ottobre 2023, è divenuto, a decorrere dal 2 gennaio 2024, il modello generalizzato per la gestione telematizzata dell'intera fase delle indagini preliminari⁹⁹.

Più nello specifico, si è al cospetto di un sistema informatico progettato non tanto per sostituire il modello TIAP attualmente esistente, bensì onde consentire a tutti i soggetti abilitati la redazione in formato digitale, la firma elettronica e il deposito telematico degli atti dal momento della ricezione della notizia di reato, rendendo così telematici tutti i flussi procedurali. L'applicativo, dunque, vorrebbe realizzare quel passaggio, che rappresenta il vero fulcro dell'informatizzazione, dalla dematerializzazione alla digitalizzazione degli atti, ovverosia da un sistema di gestione dei fascicoli incentrato sulla semplice scansione degli atti

97. Ai sensi dell'art. 2 comma 1, lett. m), n. 2 del d.m. n. 44/2011, i soggetti abilitati interni sono i magistrati, il personale degli uffici giudiziari e degli UNEP.

98. A mente del quale «rimane consentito il deposito mediante posta elettronica certificata come disciplinato dall'articolo 87-*bis* del decreto legislativo 10 ottobre 2022, n. 150 per tutti i casi in cui il deposito può avere luogo anche con modalità non telematiche».

99. IANNONE 2024; SAVIO 2024.

processuali cartacei a un modello governato interamente da file nativi digitali.

Con riguardo all'ambito di operatività del nuovo sistema, occorre fare riferimento al già citato d.m. n. 271/2023, il quale prevede l'obbligatorietà del deposito telematico tramite APP di «atti, documenti, richieste e memorie» nei soli «procedimenti di archiviazione di cui agli articoli 408, 409, 410, 411 e 415 del codice di procedura penale nonché alla riapertura delle indagini di cui all'articolo 414 del codice di procedura penale» a decorrere dal 14 gennaio 2024. A partire da quella data, dunque, tutte le fasi della procedura archiviativa (dall'invio della richiesta all'adozione del provvedimento conclusivo) e di quella concernente la riapertura delle indagini debbono essere gestite telematicamente.

Tanto premesso sul piano teorico, va rilevato come la prima fase di sperimentazione operativa dell'applicativo sia risultata fallimentare. A riprova di ciò basti pensare che, secondo quanto riportato dal CSM, gli uffici giudiziari hanno riscontrato profili di criticità talmente numerosi nell'uso di APP da rendere lo strumento «inidoneo ad essere utilizzato [in qualunque fase del procedimento]»¹⁰⁰.

Tra i numerosi deficit del sistema segnalati vi erano (e vi sono tutt'ora), innanzitutto, quelli legati alla sicurezza. A quanto è dato rilevare, il funzionamento del software, acquisendo i profili utente da quelli presenti sul SICP, consente al singolo magistrato di visualizzare tutti i fascicoli caricati nel sistema, compresi, dunque, pure quelli dei colleghi, potendo egli teoricamente modificare o eliminare provvedimenti contenuti in procedimenti assegnati ad altri magistrati dell'ufficio. È evidente come la mancata previsione di misure tecniche idonee a garantire la sicurezza e la riservatezza dei dati giudiziari non possa che lasciare alquanto perplessi, ancor più se si considera che la riforma Cartabia, come si desume da una lettura sistematica delle numerose disposizioni neo-introdotte¹⁰¹, individua proprio nel requisito della «segretezza» degli atti e dei documenti una *conditio sine qua non* «di

attuazione dei principi e dei diritti fondamentali che innervano il processo penale»¹⁰².

A fronte di tale quadro, risulta davvero paradossale anche la problematica tecnica riscontrata con riguardo al canone della «accessibilità», pure elevato teoricamente dal legislatore del 2022 a pilastro dell'intera disciplina del «rito 2.0». Si allude al fatto che, stando al funzionamento di tale applicativo, al pubblico ministero è inibito il potere di iscrivere autonomamente un nuovo procedimento penale o di adottare provvedimenti, anche in casi di urgenza (si pensi ad un decreto di intercettazione), in assenza della validazione di un cancelliere.

Le problematiche strutturali di APP non finiscono però qui. Appaiono insufficienti, del pari, i modelli standard degli atti processuali e dei provvedimenti inseriti di *default* nello strumento, né è prevista la possibilità per il singolo magistrato di sopperire a tale mancanza. Per di più, la creazione dei documenti passa per il tramite di un *wizard*, cioè una procedura guidata di redazione, che non consente all'utente di discostarsi da essa, neppure quando, come è stato rilevato in alcune occasioni, quest'ultima dia esiti giuridicamente erronei¹⁰³.

Ancora: APP non consente un'interazione contestuale di più utenti sul medesimo fascicolo, inibendo, perciò, la possibilità di redigere e modificare contemporaneamente atti in relazione allo stesso procedimento.

Quel che è peggio è che l'applicativo in parola, in aggiunta, non sembra neppure in grado, così per come modellato dagli ingegneri informatici, di sfruttare appieno le potenzialità offerte dalla tecnologia. Emblematica si rivela, ad esempio, la mancata predisposizione di un idoneo scadenziario delle misure cautelari e di un corrispondente *alert* dei termini in scadenza.

Ebbene, va osservato che le problematiche pratico-applicative di cui abbiamo dato brevemente conto hanno avuto importanti riflessi sulla concreta gestione delle procedure, specie sul versante delle loro tempistiche, giacché, a quanto è dato

100. Così si esprime la *Relazione del CSM sulla sperimentazione in esercizio del sistema APP 1.0*, 19 novembre 2023, p. 3. Cfr. pure la Delibera plenaria del CSM del 13 marzo 2024, *Criticità relative all'applicativo APP rilevate dagli Uffici giudiziari*.

101. Artt. 110, 111-bis, 111-ter, 148 c.p.p.

102. Testualmente, SIGNORATO 2023, p. 67, la quale, con una formula assai felice, soggiunge come «la sicurezza dei dati funge da presupposto per la sicurezza dei diritti».

103. Ne dà conto SAVIO 2024, par. 1.

sapere, per realizzare la medesima attività (ad es., la redazione di una richiesta di archiviazione), in molti casi il soggetto abilitato (pubblico ministero, gip, cancelliere, etc.) rischia di impiegare più tempo utilizzando APP rispetto a una gestione cartaceo-analogica¹⁰⁴. Onde rendersi conto di un tanto, è sufficiente volgere lo sguardo alle statistiche giudiziarie¹⁰⁵: i dati raccolti per il tramite della rete RID, che attualmente riguardano 114 Procure su 140, rivelano un calo del 63,7 % nel numero delle richieste di archiviazione nei procedimenti a carico di noti e dell'80,1 % per i procedimenti nei confronti di persone ignote¹⁰⁶. Per quanto concerne gli Uffici giudicanti, invece, il dato rilevato, che riguarda 98 uffici GIP su 140, mostra un calo del 93,4 % dei decreti di archiviazione nei procedimenti mod. 21 e del 96,9 % di quelli a mod. 44¹⁰⁷. Questi dati consentono di svolgere una duplice considerazione: per un verso, essi si pongono in evidente controtendenza rispetto agli obiettivi di riduzione dei tempi processuali fissati dal legislatore; per altro verso, essi dimostrano come le nuove tecnologie, pur avendo indiscutibili potenzialità, se non adeguatamente valorizzate, possano trasformarsi in un'arma a doppio taglio, rendendo financo più complessa la gestione dell'intero apparato giudiziario.

A fronte di tale scenario¹⁰⁸, dunque, non devono sorprendere i numerosi provvedimenti adottati dal DGISIA in sede nazionale e dai singoli dirigenti degli uffici a livello locale¹⁰⁹ con i quali, facendo

leva sul *dictum* dell'art. 175-bis c.p.p., si è certificato il malfunzionamento di APP e, di conseguenza, reso legittimo il ricorso al regime analogico, specie per la realizzazione dei depositi. Emblematici si rivelano, al riguardo, due provvedimenti adottati a distanza di poche settimane (29 marzo 2024 e 31 maggio 2024) dal Presidente del Tribunale di Milano¹¹⁰ (notoriamente uno degli uffici giudiziari più all'avanguardia sul versante della digitalizzazione), il quale ha disposto la sospensione dell'utilizzo di APP fino a data da destinarsi, consentendo agli uffici di gestire in modalità cartacea tutte le fasi del procedimento archiviativo.

Per concludere sul punto, ci pare che le numerose criticità emerse dall'utilizzo quotidiano del meccanismo siano da ricondurre a un erroneo approccio al tema. L'impressione, invero, è che il "legislatore tecnico" si sia completamente disinteressato della realtà giudiziaria e, in particolare, del funzionamento e delle peculiarità dei singoli uffici nei quali lo strumento tecnologico (nel caso di specie, APP) deve essere impiegato. Lo sviluppo di un *tool* che non tiene in debito conto delle apparecchiature informatiche concretamente disponibili, dell'articolazione interna dell'ufficio e, perché no, delle *skills* digitali degli operatori, non può che rivelarsi del tutto inefficace o, come nel caso di APP, financo dannoso¹¹¹.

104. SAVIO 2024, par. 1: «APP si rivela in grado di poter rallentare tutte le attività processuali appesantendole di passaggi non necessari». Pure il Procuratore della Repubblica presso il Tribunale di Napoli ha dichiarato che «il tanto annunciato processo penale telematico non è una realtà. L'applicativo App non funziona o funziona molto lentamente».

105. Le statistiche sono reperibili nel sito del CSM.

106. In termini assoluti, la rilevazione, che riguarda l'81,4% degli uffici, denuncia il calo di 35.504 richieste a mod. 21 e 100.910 richieste a mod. 44 rispetto allo stesso periodo del 2023.

107. In termini assoluti in poco più di un mese il calo delle archiviazioni è stato di 43.455 procedimenti a carico di noti e di 101.696 a carico di ignoti.

108. Invero, deve darsi conto di come, a seguito di numerose segnalazioni provenienti dagli operatori del diritto, il Ministero abbia provveduto ad aggiornare alcune componenti del sistema.

109. Cfr., ad es., Procura di Tivoli, 18 aprile 2024; Procura e Tribunale di Taranto, 13 febbraio 2024; Procura di Bari, 24 febbraio 2024.

110. I provvedimenti sono reperibili su: Provvedimento del 29 marzo 2024; Provvedimento del 31 maggio 2024.

111. CONSIGLIO NAZIONALE DI MAGISTRATURA DEMOCRATICA, APP: uno strumento inidoneo che chiama in causa l'inadeguatezza del Ministero, impone un ruolo attivo al CSM, richiede una riflessione della magistratura associata, 6 febbraio 2024.

6. Le notificazioni 2.0

Nella prospettiva di una maggiore efficienza processuale, la riforma Cartabia non si è accontentata di ridisegnare la disciplina della formazione e del deposito degli atti processuali, ma ha giustamente approntato una ristrutturazione complessiva pure del sistema delle notificazioni¹¹². La convinzione di fondo, espressa a chiare lettere dai *conditores*, era quella per cui l'ingranaggio in parola rappresentasse uno dei «principali fattori di dilatazione del processo e di reiterazione di atti, con conseguente allungamento dei tempi, approssimarsi della prescrizione e disfunzioni per tutti i soggetti coinvolti nel processo»¹¹³.

Alla luce di ciò, ben si comprende il motivo per il quale il legislatore abbia individuato nell'impiego degli strumenti digitali il principio reggente l'intera disciplina. Le notificazioni – recita il nuovo art. 148, comma 1, c.p.p. – devono avvenire, di regola, in modalità esclusivamente telematica, assicurando, a pena di nullità *ex art.* 171, comma 1, lett. b-bis, c.p.p., l'identità del destinatario e del mittente, l'integrità del documento trasmesso e la certezza, anche temporale, dell'avvenuta trasmissione e ricezione. Pure in questa circostanza, il legislatore non precisa quali debbano essere gli strumenti informatici da impiegare, rinviando, a tal fine, ad altre fonti secondarie.

Al netto di altre modifiche aventi carattere più circoscritto¹¹⁴, è senz'altro alla disciplina concernente le notificazioni all'imputato non detenuto

che il legislatore ha dedicato maggiore attenzione; e ciò nel tentativo – non del tutto riuscito – di evitare che la svolta tecnologica finisse per produrre «frutti avvelenati», comprimendo i sovraordinati diritti difensivi dei prevenuti.

In proposito, con riguardo alla prima comunicazione di atti diversi da quelli contenenti la *vocatio in iudicium* – rispetto ai quali è stata prevista una disciplina *ad hoc* nell'art. 157-ter c.p.p. –, la lettura congiunta degli artt. 157 e 161, comma 1, c.p.p. impone, in particolare, di procedere mediante consegna di copia dell'atto in forma di documento analogico. Al momento della notificazione, inoltre, il comma 8-ter dell'art. 157 obbliga l'autorità ad avvertire l'imputato che le comunicazioni successive – diverse da quelle contenenti la *vocatio* – saranno sempre e comunque effettuate al difensore di fiducia o d'ufficio.

Questo residuo spazio alle notificazioni non digitali, tuttavia, può trovare applicazione solamente ove sussistano, congiuntamente, due requisiti.

Innanzitutto, a), il riferimento ai «casi di cui all'art. 148, comma 4, c.p.p.» contenuto nell'*incipit* dell'art. 157 c.p.p., impone di procedere attraverso le predette modalità analogiche se e solo se la notifica telematica non possa essere effettuata «per espressa previsione di legge, per l'assenza o l'inidoneità di un domicilio digitale o per la sussistenza di impedimenti tecnici». In tutte le altre ipotesi, la prima notifica va effettuata con modalità telematiche¹¹⁵.

112. CIMADOMO 2023; COLAIACOVO 2023; GIORDANO 2022; NARDO 2023; NICOLICCHIA 2023.

113. *Relazione illustrativa al d.d.l. A.C. 2435*, p. 3.

114. Concernenti, in particolare, le notificazioni all'imputato detenuto, all'imputato residente all'estero, nonché all'irreperibile, al latitante, all'evaso, e alle parti private.

115. Al riguardo, due precisazioni appaiono necessarie. La prima. Il concetto di «domicilio digitale» si riferisce, così come stabilito dall'art. 1, comma 1, lett. n-ter) del d.lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale – CAD), all'indirizzo di posta elettronica certificata (PEC), valido ai fini delle comunicazioni elettroniche aventi valore legale. La seconda. «L'idoneità» della PEC, a fini processuali, è subordinata, a norma dell'art. 16-ter d.l. 18 ottobre 2012, n. 179, al fatto che essa debba risultare dai pubblici elenchi. L'art. 2, comma 5 CAD, infatti, prevede che le disposizioni ivi contenute trovino applicazione pure con riguardo «al processo civile, penale, amministrativo, contabile e tributario». Di conseguenza, laddove il domicilio digitale, pur esistente, non risulti dai pubblici registri, esso deve ritenersi inidoneo per il perfezionamento della prima notifica. Diverso è, però, il caso in cui, in ossequio a quanto previsto all'art. 161, comma 1, c.p.p., l'indagato, a seguito del primo contatto con l'autorità procedente e ricevuto apposito invito, scelga volontariamente e consapevolmente di dichiarare un «domicilio telematico», ovverosia «un indirizzo di posta elettronica certificata [non risultante da pubblici registri]»: in tale circostanza, tutte le notificazioni avverranno a mezzo PEC, anche se l'indirizzo non risulta inserito nei pubblici registri.

Ulteriore requisito di operatività, *b*), è la mancata comunicazione degli avvertimenti previsti all'art. 161, comma 01, c.p.p. La disposizione, infatti, prevede che la polizia giudiziaria, nel primo atto compiuto con l'intervento dell'indagato, debba avvertire quest'ultimo che le successive notificazioni saranno effettuate al difensore di fiducia o d'ufficio.

Per quanto concerne, invece, le notificazioni successive alla prima, l'art. 157-*bis* c.p.p. stabilisce che queste vadano sempre eseguite all'indirizzo PEC del difensore di fiducia o d'ufficio. In tale ultimo caso, però, la disposizione introduce un regime derogatorio, prevedendo che queste debbano essere effettuate a norma dell'art. 157 c.p.p. (cioè a dire, con modalità analogiche) qualora: *i*) l'indagato non abbia ricevuto gli avvisi di cui agli artt. 161, comma 1, c.p.p. o quelli di cui all'art. 157, comma 8-*ter*, c.p.p. e *ii*) la prima notifica sia avvenuta mediante consegna di copia dell'atto a persona diversa dallo stesso indagato o da persona che con lui coabita ovvero, ancora, al portiere.

Infine, in ragione dell'importanza assunta dall'istituto, il legislatore ha approntato una regolamentazione specifica per le notificazioni degli atti di *vocatio in iudicium*. Il neo-introdotta art. 157-*ter* c.p.p. prevede, al riguardo, che il decreto di fissazione dell'udienza preliminare, il decreto di citazione a giudizio di cui agli artt. 450, comma 2, 456, 552 e 601 c.p.p. e il decreto penale di condanna vadano trasmessi all'indagato nel proprio domicilio dichiarato o eletto ai sensi dell'art. 161, comma 1, c.p.p. anche telematico. In mancanza, soccorrono le modalità tradizionali previste dall'art. 157 c.p.p. La scelta a favore di un regime di tal fatta è da rintracciarsi nella delicatezza che connota questo tipo di comunicazione: essendo quest'ultima prodromica all'esercizio del diritto sovraordinato di partecipare al procedimento, si è voluta individuare la modalità maggiormente capace di assicurare all'imputato la conoscenza effettiva circa la pendenza del processo a suo carico.

7. La nuova disciplina organica della partecipazione a distanza

Come si è anticipato, il secondo macro-filone di modifiche in tema di digitalizzazione operate dalla novella ha avuto a oggetto il profilo della disciplina in tema di udienze da remoto. In proposito, con il dichiarato intento di non abbandonare l'esperienza maturata nel corso della pandemia in merito all'impiego di collegamenti esterni all'aula fisica di udienza, già la Commissione ministeriale incaricata di strutturare la novella (cd. Commissione Lattanzi) aveva messo in luce i benefici che possono derivare da una gestione razionale della cd. *remote justice*: l'informatizzazione di talune attività processuali – si è sottolineato – sarebbe in grado di assicurare non solo «maggiore efficienza e rapidità al procedimento penale, ma anche [di] incrementare le garanzie della difesa»¹¹⁶.

Facendo seguito a queste indicazioni, ai sensi dell'art. 1, comma 8, lett. b), della l. n. 134/2021, il Governo era delegato, in particolare, a «individuare i casi in cui, con il consenso delle parti, la partecipazione all'atto del procedimento o all'udienza possa avvenire a distanza». Va, in proposito, ricordato che la formulazione del criterio direttivo, era stata condivisibilmente criticata dai primi commentatori, i quali ne avevano subito evidenziato l'eccessiva genericità: si era affermato, in particolare, che «il livello di precisione del [medesimo] era] inversamente proporzionale alla delicatezza dell'istituto»¹¹⁷. A parte tale difetto strutturale, a non convincere era, in particolare, il mancato riferimento ai principi generali (ad eccezione del «consenso delle parti») che avrebbero dovuto guidare il Governo in sede di attuazione: nessun cenno veniva operato, ad esempio, al necessario rispetto dei canoni di immediatezza, di pubblicità e al contraddittorio nella formazione della prova. Emblematico appare, in tal senso, il mancato richiamo – previsto, invece, nella bozza elaborata dalla Commissione Lattanzi¹¹⁸ – alla necessità di garantire il «diritto di difesa».

Facendo, almeno parziale, tesoro di tali critiche, il Governo, in sede di attuazione della delega, non si è limitato a «individuare» i singoli casi di

116. *Relazione finale e proposte di emendamenti al d.d.l. A.C. 2435*, p. 16. Si veda, sul punto, LASAGNI 2023.

117. DI PAOLO 2022, p. 102. Nello stesso senso, v. DEI-CAS 2022, p. 6.

118. In specie, nell'art. 2-*quater* della *Relazione finale e proposte di emendamenti al d.d.l. A.C. 2435*, p. 15.

intervento da remoto¹¹⁹, bensì ha opportunamente introdotto una disciplina generale e organica della partecipazione a distanza. Ed è proprio in questa prospettiva che il nuovo Titolo II-*bis* del Libro II del codice di procedura penale contiene oggi due disposizioni, gli artt. 133-*bis* e 133-*ter*, rispettivamente dedicate all'identificazione dell'ambito applicativo della normativa e al riconoscimento esplicito di talune garanzie processuali essenziali della materia. La scelta di predisporre un modello generale cui fare ricorso ogniqualvolta le parti siano chiamate a svolgere un'attività da remoto si lascia, evidentemente, apprezzare, dal momento che mira a coniugare le esigenze di tutela dei diritti fondamentali dell'individuo con la necessità di sfruttare quello che nell'attuale contesto storico è divenuto uno strumento utile all'esercizio della giurisdizione¹²⁰.

Entrando nel merito della disciplina normativa, va ricordato che l'art. 133-*bis* c.p.p. stabilisce che, salvo diversa disposizione di legge, la nuova disciplina sul collegamento da remoto (dettagliatamente regolata all'articolo successivo) debba trovare applicazione ogniqualvolta «l'autorità giudiziaria dispone che un atto sia compiuto a distanza o che una o più parti possano partecipare a distanza al compimento di un atto o alla celebrazione di un'udienza».

Due sono le considerazioni che vanno compiute al riguardo.

In prima battuta, va detto che il tenore letterale della norma induce a conferirle una portata generale, onde per cui la regolamentazione di recente

conio deve ritenersi applicabile a tutte le ipotesi di *remote justice* previste dalla legge, pure se già contenute nelle disposizioni di attuazione al codice di rito (si pensi, ad esempio, agli artt. 146-*bis* e 146-*ter*, disp. att. c.p.p., che sono rimasti in vigore)¹²¹.

In secondo luogo, è degno di nota il fatto che tra i casi presi in considerazione siano annoverate differenti attività procedimentali, ovverosia la partecipazione: *i*) a un «atto» del procedimento, quale, ad esempio, l'interrogatorio di garanzia, le sommarie informazioni dell'indagato o l'audizione dell'interessato sottoposto a misura cautelare nel procedimento di estradizione¹²²; *ii*) a un'udienza telematica.

Con riguardo a quest'ultima ipotesi, è opportuno chiedersi se il dettame testuale dell'art. 133-*bis* c.p.p. autorizzi o meno lo svolgimento di forme «estreme» di udienze del tutto smaterializzate. In proposito, del resto, è ormai nota la differenza che intercorre tra la c.d. *virtual hearing*¹²³ e l'udienza a distanza *lato sensu* intesa: mentre nel primo caso nessuno dei protagonisti processuali condivide uno spazio fisico comune, nel secondo, invece, la partecipazione a distanza è consentita solamente ad alcuni soggetti del procedimento (tendenzialmente, le parti private e, talvolta, pure il pubblico ministero). Questa distinzione non è priva di rilievo, giacché solo nella prima ipotesi, a ben vedere, si è al cospetto di un «modello a smaterializzazione diffusa»¹²⁴, espressione di quel più generale fenomeno descritto in termini di «despazializzazione totale» delle attività processuali¹²⁵. Nelle restanti situazioni, invece, il rito penale mantiene, almeno

119. Per una compiuta enumerazione delle varie ipotesi in cui è possibile procedere a distanza, v. PORCU 2022, pp. 92-96.

120. Per tali considerazioni, v. GIALUZ 2022, p. 21 ss.

121. Nello stesso senso, GALGANI 2023-C; GIALUZ 2022, p. 22; TRIPICCIÓN 2022.

122. Cfr. rispettivamente, gli artt. 294, comma 4, 350, comma 4-*bis*, 717, comma 2, c.p.p.

123. SUSSKIND 2019, p. 359, la definisce come l'ipotesi nella quale «nessuno dei protagonisti processuali condivide uno spazio fisico comune» (trad. nostra). Cfr. pure DI PAOLO 2022, p. 102.

124. LORUSSO 2020, par 2.

125. GARAPON 2021; DANIELE 2021, p. 62, per il quale, in dette ipotesi, si assiste a una «rottura più totale delle normali coordinate spaziali e sensoriali delle udienze». Come sottolinea anche DI CHIARA 2018, p. 1483, «l'aula di udienza non ha più "sede" nella fisicità di uno spazio unico, continuo, segnabile su una mappa, ove gli attori della performance giudiziaria siedono, intervengono, si muovono, ma diviene anch'essa aula di udienza estesa; la postazione fisica (un tempo) centrale – l'aula ospitata a Palazzo di Giustizia, censita sulla mappa dell'immobile, segnata nei piani antincendio della struttura architettonica – conquista dimensioni nuove componendosi in un ensemble che comprende una o più postazioni remote, che dialogano con il theatrum centrale attraverso collegamenti costituiti da reti informatiche».

in parte, la propria “materialità”, dal momento che il giudice è chiamato a esercitare il potere giurisdizionale nell’aula (fisica) del tribunale.

Tanto premesso, va chiarito che l’attuale costruito normativo sembra giustificare soltanto la realizzazione di udienze parzialmente telematiche¹²⁶. L’art. 133-*bis* c.p.p., in effetti, consente la partecipazione a distanza solo di «una o più parti», di talché deve ritenersi sempre indispensabile la presenza fisica del giudice¹²⁷ nel palazzo di giustizia.

La stessa conclusione, però, non sembra potersi estendere così agevolmente pure con riguardo al rappresentante d’accusa. *Prima facie*, il divieto per quest’ultimo di collegarsi da remoto sembrerebbe giustificato dal fatto che, a differenza di quanto previsto all’art. 133-*ter*, comma 7, c.p.p. con riguardo al difensore¹²⁸, nulla viene specificato con riguardo al pubblico ministero. Ad ulteriore sostegno, inoltre, potrebbe invocarsi il dettato letterale del nuovo art. 146-*bis*, comma 4-*bis*, disp. att. c.p.p., ove ammette alla presenza via video le sole parti «private»¹²⁹. Epperò, in una prospettiva del tutto antitetica, va considerato come l’art. 133-*bis* c.p.p. – che, come detto, impiega il più generico lemma «una o più parti» – è una disposizione a “vocazione generalizzata”, destinata a trovare applicazione, ad eccezione dell’ipotesi contemplata nelle disposizioni di attuazione, in tutte le altre situazioni in cui la legge ammette forme di partecipazione a distanza.

Va infine osservato come il neo introdotto art. 133-*ter* c.p.p. – oltre a prevedere una regolamentazione puntuale del diritto di informazione dei soggetti interessati, nonché sull’individuazione del luogo di collegamento delle parti – predisponga

una serie di garanzie, presidiate dalla sanzione della nullità. Si tratta, in particolare, di quei presidi a tutela di un’effettiva e consapevole partecipazione al processo individuati dalla Corte costituzionale nella già richiamata pronuncia n. 342 del 1999: salvaguardia del contraddittorio ed effettività della partecipazione (si legga, idoneità dei mezzi tecnici) sono, dunque, principi di carattere generale ad “applicazione diffusa”, ovvero sia valevoli per qualsivoglia ipotesi di partecipazione remota. Anche sotto tale profilo, però, la riforma mostra luci e ombre: se, per un verso, appare del tutto condivisibile l’opera di codificazione delle garanzie minime indicate dalla Consulta, per altro verso, non può non riconoscersi come ciò appaia, per certi aspetti, insufficiente. In effetti, pure a fonte di strumentazioni tecniche idonee a tutelare una piena e consapevole partecipazione all’atto o all’udienza, l’esercizio del diritto di difesa e del contraddittorio, in quanto mediati dallo schermo, si rivelano essere, in un certo qual modo, “imperfetti” e “attenuati”¹³⁰, dal momento che «la presenza digitale, “*in imagine*”», come si è osservato, risulta «ontologicamente diversa da quella “*in corpore*”»¹³¹.

8. Auspici per il futuro

L’analisi di un tema come quello della digitalizzazione della giustizia penale non permette di formulare delle conclusioni “definitive”. Se, infatti, la tecnologia informatica, come osservato dai più autorevoli studiosi¹³², è un fenomeno in continua evoluzione, anche la scienza giuridica che con essa si confronta non può che essere caratterizzata dalla stessa dinamicità.

126. Si mostra critico rispetto a questa scelta del legislatore, GIALUZ 2022, p. 23. Negli stessi termini pure GALGANI 2023-C, p. 1182.

127. Nulla è specificato con riguardo agli ausiliari (cancellieri e Addetti all’Ufficio per il processo). Alla luce delle funzioni di assistenza svolte da questi ultimi, però, sembra ragionevole prospettare una forma di partecipazione speculare a quella prevista per il giudice.

128. Il quale può collegarsi dal proprio ufficio o da altro luogo, purché idoneo.

129. A sostegno di questa esegesi, v. GALGANI-AGOSTINO 2024, p. 228; NEGRI 2023, p. 475.

130. DANIELE 2012, p. 247. Cfr. pure CURTOTTI NAPPI 2006, pp. 301, 305, ove si sottolinea come, nel caso del “telesame”, il problema non sta tanto nel domandarsi se questa modalità di acquisizione della prova comprometta le garanzie processuali, bensì nel chiedersi se questa «anomalia riesca comunque a preservare il “nucleo garantista minimo”» dei precetti costituzionali. Di «un inevitabile gap» tra la partecipazione in presenza e la connessione a distanza parla DI CHIARA 2018, p. 1490.

131. DANIELE 2021, p. 65.

132. FLORIDI 2017.

Ciò nondimeno, alcuni punti fermi possono comunque essere individuati.

Anzitutto, il presente lavoro ha avuto modo di dimostrare come, effettivamente, la riforma Cartabia abbia segnato, in questo settore, un deciso cambio di passo. Nel dare seguito alle ormai numerose indicazioni provenienti dalle fonti sovranazionali, si è scelto, in maniera del tutto condivisibile, di procedere con una “massiccia” informatizzazione di ogni fase del procedimento penale, perseguendo quale obiettivo quello di creare così una realtà giudiziaria finalmente *paperless*. Entrambe le aree di intervento (processo penale telematico in senso stretto e partecipazione a distanza) sembrano accomunate da una visione unitaria di fondo: se è vero, come ha osservato autorevole dottrina¹³³, che la tecnologia è sempre e solo un mezzo e mai un fine, ne consegue che il “passaggio al digitale”, lungi dal dover rappresentare un mantra da perseguire ad ogni costo, deve essere valorizzato solo in quei casi in cui sia capace di aggiungere un *quid pluris* rispetto a una gestione cartaceo-centrica; cioè, a dire, un innalzamento delle garanzie e, contestualmente, una maggiore rapidità delle procedure. E che la via intrapresa sia quella giusta è confermato, in termini espliciti e inequivoci, dall'ultimo *Rule of Law Report - 2024* elaborato dalle istituzioni europee, ove può leggersi come la recente novella abbia prodotto «some further progress on continuing the efforts to further improve the level of digitalisation for criminal courts and prosecutors' offices»¹³⁴.

Che quanto fatto dalla riforma Cartabia rappresenti, però, solo di un punto di partenza è un dato altrettanto difficile da negare: ciò è, del resto, provato dall'*EU Justice Scoreboard 2024*, ove, infatti, l'Italia si attesta ancora negli ultimi posti tra i Paesi dell'Unione in termini di implementazione di soluzioni digitali nei procedimenti penali.

Ora, se è vero che a quest'ultimo dato non deve attribuirsi un'importanza decisiva – giacché il processo di compiuta entrata a regime dell'opera di telematizzazione dell'apparato giudiziario nazionale è ancora in corso – ci sembra, in ogni caso, che la via prescelta dai riformatori, benché

“lastricata di buone intenzioni”, rischi di presentare comunque ancora gravi limiti.

Al riguardo, va, anzitutto, osservato come uno sguardo d'insieme ai numerosi report e pareri provenienti dalle varie associazioni di categoria – ma, ancor prima, la più semplice frequentazione delle aule di giustizia – ci consegna un quadro operativo ancora spesso desolante, nel quale le previsioni codicistiche faticano a trovare concreta attuazione nella prassi quotidiana, a causa, *in primis*, delle note carenze strutturali che caratterizzano molti uffici giudiziari. La distanza tra *law in the book* e *law in action* risulta, insomma, da questa prospettiva ancora più evidente.

Ad aggravare la situazione sta poi il fatto che all'insufficienza delle apparecchiature informatiche, sia dal punto di vista quantitativo sia qualitativo, si somma l'inadeguatezza tecnica del modo in cui molti software, che dovrebbero facilitare il lavoro di tutti gli attori del processo, sono stati concepiti e sviluppati. I menzionati *bug* relativi al funzionamento di APP e il mancato coordinamento tra le diverse infrastrutture informatiche allo stato in uso presso gli uffici giudiziari danno, del resto, ampia conferma di tale assunto. L'impressione è, insomma, che il “formante tecnologico” non sia finora stato configurato in modo adeguato onde dare attuazione al più avanzato “formante codicistico”.

Per di più, non sembra che, allo stato attuale, il legislatore abbia investito a sufficienza neppure nel “capitale umano”, né sotto il profilo della “formazione digitale” dei cancellieri e di tutti coloro che quotidianamente con essi collaborano (si pensi, ad esempio, agli addetti all'ufficio per il processo¹³⁵), né con riguardo all'assunzione di personale informatico specializzato.

Tutto ciò ci porta ad auspicare che il “legislatore tecnico”, nel dare esecuzione ai principi fissati a livello normativo, muova nel prossimo futuro da un più attento e ponderato studio delle attività realizzate quotidianamente da magistrati, avvocati e cancellieri, al fine di comprendere non solo “che cosa” fanno, «ma [...] come lo fanno, con quali

133. GIALUZ 2022.

134. *Rule of Law Report Country Chapter on the rule of law situation in Italy*, 24 July 2024, p. 2.

135. Sul punto, v. MIRAGLIA 2024; e, con specifico riguardo al ruolo che ad essi potrebbe essere attribuito nell'ambito di una nuova “cultura digitale dell'organizzazione giudiziaria”, sia consentito il rinvio ad MALACARNE 2024.

tempi, e con quali relazioni con soggetti interni ed esterni agli Uffici»¹³⁶.

Ma non è tutto. È opportuno mettere in luce quello che è probabilmente il maggiore aspetto deficitario della riforma in materia di nuove tecnologie: si allude, in particolare, alla circostanza per cui i *conditores* non abbiano sfruttato la grande occasione fornita dalla novella in esame per affrontare pure i plurimi nodi problematici, recentemente acuiti dell'approvazione del Regolamento europeo sull'intelligenza artificiale¹³⁷, che affliggono la disciplina italiana dei mezzi di prova e di ricerca della prova tecnologici. Se è vero, infatti, che il legislatore era stato chiamato ad operare su un testo già in parte “bloccato” dalle contrapposizioni politiche, che caratterizzavano le fragili maggioranze della precedente legislatura, deve comunque censurarsi la scelta di disinteressarsi completamente del profilo, cruciale per le odierne società dell'informazione, della regolazione degli strumenti di controllo occulto degli individui e della collettività tramite device tecnologici.

Non è un mistero, del resto, che il nostro ordinamento continua, anche a valle della riforma Cartabia, a non disciplinare del tutto un ampio novero di forme di *digital investigation* oggi essenziali per il contrasto alla criminalità¹³⁸. Il riferimento corre, ad esempio, al pedinamento GPS¹³⁹, alle videoriprese investigative¹⁴⁰, all'impiego di algoritmi di riconoscimento facciale e del *virus trojan*, utilizzato in modalità diversa rispetto alla semplice captazione ambientale¹⁴¹. Il carattere occulto e la capacità di immagazzinare una quantità enorme di dati e informazioni rendono, invero, questi strumenti altamente appetibili per l'autorità inquirente, giacché consentono di ottenere “la massima resa con il minimo sforzo”. Epperò, la persistente assenza

di una disciplina legislativa chiara e precisa in materia genera evidenti frizioni, *in primis*, con il principio di legalità processuale (art. 111, comma 1, Cost.), dal momento che finisce per rimettere alla prassi (*rectius*, agli ondivaghi orientamenti giurisprudenziali) l'indicazione dei presupposti circa l'impiego di *tool* altamente intrusivi. Ma, va detto, la mancanza di una disciplina adeguata sul punto determina problemi ancor più profondi: è evidente, infatti, come le lacune della disciplina in materia compromettano alla base la stessa possibilità di assicurare un adeguato bilanciamento tra esigenze di salvaguardia di plurimi diritti fondamentali dell'uomo (come quelli alla difesa, alla parità delle parti, al contraddittorio, così come al rispetto della vita privata e alla protezione dei dati personali), da un lato, e di contrasto alla criminalità, da un altro lato.

A fronte di ciò, risulta evidente la necessità di compiere ancora un ulteriore cambio di passo in materia di rapporto tra digitalizzazione e *criminal procedure*, rispetto a quello compiuto dalla riforma Cartabia sotto il profilo del processo penale telematico *lato sensu* inteso. È quantomai urgente completare il percorso di transizione tecnologica del sistema approntando finalmente una serie di previsioni volte a regolare, in modo organico, pure la pletora di strumenti di indagine e di prova tecnologici impiegati nella realtà giudiziaria. Bisogna, del resto, essere ben consapevoli che, finché non vi saranno norme che individuino i casi, i modi e i limiti di utilizzo di siffatti strumenti, vi sarà sempre il rischio, quantomai elevato, che le esigenze di lotta ai reati finiscano per tiranneggiare rispetto a quelle di protezione della persona, aprendosi finanche le porte a scenari orwelliani, incompatibili con i più basilari principi su cui dovrebbero reggersi le democrazie contemporanee¹⁴².

136. SAVIO 2024, par. 3.

137. Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale.

138. In generale, sulla necessità di un intervento legislativo volto a regolamentare queste nuove strumentazioni investigative, v., pur con differenti accentuazioni e prospettive di riforma, BENE 2019; GIALUZ 2020; MARCOLINI 2015; MIRAGLIA 2023, NICOLICCHIA 2020; NOCERINO 2021, p. 317 ss.; ORLANDI 2014.

139. BENE 2019; SIGNORATO 2012; FANUELE 2019.

140. Sul tema, come noto, la letteratura è sconfinata: per reperire i dovuti riferimenti dottrinali, cfr. BONINI 2019; TRIGGIANI 2019; oltre alla voce di CAMON 2013.

141. Cfr. GRIFFO 2019; NOCERINO 2021; TORRE 2017. Per una recente ed approfondita sintesi, v. MIRAGLIA 2023.

142. Come si è avuto modo di rilevare in altra sede, ci pare che un ruolo propulsivo chiave al riguardo avrebbe potuto essere assunto, al riguardo, dal Comitato tecnico-scientifico per la digitalizzazione della giustizia penale, di

Riferimenti bibliografici

- E. AMODIO (2022), *La cultura della speditezza processuale nella riforma Cartabia*, in “Rivista italiana di diritto e procedura penale”, 2022, n. 1
- E. AMODIO (2020), *Smettiamo di storpiare l'italiano con il lugubre “da remoto”*, in “Sistema penale”, 28 aprile 2020
- E. AMODIO (2003), *La procedura penale dal rito inquisitorio al giusto processo*, in “Cassazione penale”, 2003, n. 4
- E. AMODIO, E.M. CATALANO (2020), *La resa della giustizia penale di fronte alla bufera del contagio*, in “Sistema penale”, 2020, n. 5
- T. BENE (2019), *Il pedinamento elettronico: tecnica investigativa e tutela dei diritti fondamentali*, in A. Scalfati (a cura di), “Le indagini atipiche”, Giappichelli, 2019
- V. BONINI (2019), *Videoriprese investigative e tutela della riservatezza: un binomio che richiede sistemazione legislativa*, in “Processo penale e giustizia”, 2019, n. 2
- C. BONZANO (2022), *Documentazione delle dichiarazioni: ancora incompiuto l'incerto cammino verso il sinolo aristotelico di sostanza e forma*, in G. Spangher (a cura di), “La riforma Cartabia”, Pacini Editore, 2022
- V. BOVE (2017), *La Pec a soggetti diversi dall'imputato è la forma esclusiva di notificazione o un'alternativa privilegiata*, in “IlPenalista”, 2017
- V. BOVE (2015), *Brevi riflessioni su protocolli e linee guida: è a rischio il principio di legalità?*, in “Diritto penale contemporaneo”, 2015
- S. BUZZELLI (2018), *Le modifiche alla disciplina della partecipazione a distanza*, in L. Giuliani, R. Orlandi (a cura di), “Indagini preliminari e giudizio di primo grado”, Giappichelli, 2018
- M. CAIANIELLO (2022), *Conclusive remarks. Antifraud investigations and respect for the fundamental rights faced with the challenge of e-evidence and digital devices*, in M. Caianiello, A. Camon (eds.), “Digital forensic evidence. Towards common european standards in antifraud administrative and criminal investigations”, Cedam, 2022
- M. CAIANIELLO, A. PUGLIESE (2024), *Manifesto per la giustizia penale digitale: il processo penale telematico*, in M. Caianiello, M. Gialuz, S. Quattrocchio (a cura di), “Il procedimento penale tra efficienza, digitalizzazione e garanzie partecipative”, vol. I, in G.L. Gatta, M. Gialuz, “Riforma Cartabia. Le modifiche al sistema penale”, Giappichelli, 2024
- A. CAMON (2018), *Forme, destinazione e regime della documentazione*, in G. Giostra, R. Orlandi (a cura di), “Nuove norme in materia di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche”, Giappichelli, 2018
- A. CAMON (2013), *Captazione di immagini (diritto processuale penale)*, in “Enciclopedia del diritto”, Giuffrè, 2013

cui l'art. 2, comma 20, della l. n. 134/2021 aveva previsto la possibile istituzione: sia consentito il rinvio a DELLA TORRE 2024. Purtroppo, bisogna prendere atto che tale organo è al momento rimasto solo sulla carta; essendosi così persa l'occasione di dotare l'ordinamento di una sorta di *watchdog*, in grado di svolgere la funzione, quantomai importante per le società dell'informazione contemporanee, di segnalare prontamente all'autorità il come e dove intervenire al fine di evitare che gli strumenti tecnologici da mezzi utili in chiave di efficienza, si trasformino – come nelle più cupe opere di fantascienza – in vere e proprie trappole, in grado di produrre “frutti avvelenati”.

- G. CANZIO (2021), *Le linee del modello “Cartabia”. Una prima lettura*, in “Sistema penale”, 25 agosto 2021
- G. CANZIO, F. FIECCONI (2021), *Giustizia. Per una riforma che guarda all’Europa*, Vita e Pensiero, 2021
- A. CIAVOLA (2023), *Le insidie del nuovo regime di documentazione della prova dichiarativa*, in “Processo penale e giustizia”, 2023, n. straordinario
- D. CIMADOMO (2023), *Notificazioni e “riforma Cartabia”*, in “Diritto penale e processo”, 2023, n. 1
- G. COLAIACOVO (2023), *Progressi e criticità nel nuovo assetto delle notificazioni*, in “Giurisprudenza italiana”, 2023, n. 5
- D. CURTOTTI NAPPI (2006), *I collegamenti audiovisivi nel processo penale*, Giuffrè, 2006
- D. CURTOTTI, W. NOCERINO (2024), *La transizione digitale del processo penale rimane incompiuta: una panoramica sullo stato dell’arte a margine del d.m. 217/2023*, in “La legislazione penale”, marzo 2024
- M. DANIELE (2021), *L’immediatezza in crisi. Mutazioni pericolose ed anticorpi accusatori*, in “Sistema penale”, 2021, n. 2
- M. DANIELE (2017), *La partecipazione a distanza allargata*, in “Diritto penale contemporaneo”, dicembre 2017
- M. DANIELE (2012), *La formazione digitale delle prove dichiarative. L’esame a distanza tra regole interne e diritto sovranazionale*, Giappichelli, 2012
- M. DANIELE (2011), *La prova digitale nel processo penale*, in “Rivista di diritto processuale”, 2011, n. 2
- E.A.A. DEI-CAS (2022), *La partecipazione a distanza, in attesa della riforma del processo penale*, in “Sistema penale”, aprile 2022
- J. DELLA TORRE (2024), *Il Comitato tecnico per il monitoraggio della giustizia penale e il modello di analisi statistica*, in M. Caianiello, M. Gialuz, S. Quattrocchio (a cura di), “Il procedimento penale tra efficienza, digitalizzazione e garanzie partecipative”, vol. I, in G.L. Gatta, M. Gialuz, “Riforma Cartabia. Le modifiche al sistema penale”, Giappichelli, 2024
- J. DELLA TORRE (2023), *Standard probatori, efficienza e giustizia penale*, in “Politica del diritto”, 2023, n. 3
- J. DELLA TORRE (2022), *La crisi dell’appello penale nel prisma della statistica giudiziaria*, in “Archivio penale web”, 2022, n. 2
- J. DELLA TORRE (2021), *L’espansione del processo a distanza negli itinerari dell’emergenza pandemica*, in “Processo penale e giustizia”, 2021, n. 1
- F. DELVECCHIO (2021), *L’informatizzazione della giustizia penale*, in “Diritto penale contemporaneo – Rivista trimestrale”, 2021, n. 2
- G. DI CHIARA (2018), «Come s’uno schermo». *Partecipazione a distanza, efficienza, garanzie, upgrade tecnologici*, in “Rivista di diritto processuale”, 2018, n. 6
- G. DI PAOLO (2022), *“Riforma Cartabia” e digitalizzazione del processo penale. Verso una non più rinviabile opera di ammodernamento della giustizia penale*, in “Rivista italiana di diritto e procedura penale”, 2022, n. 1
- M. DONINI (2021), *Efficienza e principi della legge Cartabia. Il legislatore a scuola di realismo e cultura della discrezionalità*, in “Politica del diritto”, 2021, n. 4
- G. DUCOLI (2023), *Registrazione audio e video*, in D. Castronuovo, M. Donini, E.M. Mancuso, G. Varraso (a cura di), “Riforma Cartabia. La nuova giustizia penale”, Cedam, 2023
- C. FANUELE (2019), *La localizzazione satellitare nelle investigazioni penale*, Cedam, 2019

- L. FILIPPI (2018), *Le nuove norme su intercettazioni e tabulati*, Pacini Editore, 2018
- L. FLORIDI (2017), *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, 2017
- B. GALGANI, L. AGOSTINO (2024), *L'impiego dei collegamenti audiovisivi ai fini della partecipazione e dell'assunzione probatoria*, in M. Caianiello, M. Gialuz, S. Quattrocchio (a cura di), "Il procedimento penale tra efficienza, digitalizzazione e garanzie partecipative", vol. I, in G.L. Gatta, M. Gialuz, "Riforma Cartabia. Le modifiche al sistema penale", Giappichelli, 2024
- B. GALGANI (2023-A), *...along came il processo penale telematico. Le disposizioni generali sugli atti*, in D. Castronuovo, M. Donini, E.M. Mancuso, G. Varraso (a cura di), "Riforma Cartabia. La nuova giustizia penale", Cedam, 2023
- B. GALGANI (2023-B), *Il processo penale telematico*, in "Diritto penale e processo", 2023, n. 1
- B. GALGANI (2023-C), *La c.d. remote justice nella riforma Cartabia*, in "Giurisprudenza italiana", 2023, n. 5
- B. GALGANI (2022), *Forme e garanzie nel prisma dell'innovazione tecnologica. Alla ricerca di un processo penale "virtuoso"*, Cedam, 2022
- B. GALGANI (2019), *Il processo penale paperless: una realtà affascinante, ancora in divenire*, in L. Luparia, L. Marafioti, G. Paolozzi (a cura di), "Dimensione tecnologica e prova penale", Giappichelli, 2019
- A. GARAPON (2021), *La despaializzazione della giustizia*, Mimesis, 2021
- G.L. GATTA (2021), *Riforma della giustizia penale: contesto, obiettivi e linee di fondo della "legge Cartabia"*, in "Sistema penale", ottobre 2021
- M. GIALUZ (2024), *Osservazioni sui correttivi alla riforma Cartabia tra rettifiche condivisibili, qualche occasione perduta e alcune sbavature*, in "Sistema penale", gennaio 2024
- M. GIALUZ (2022), *Per un processo penale più efficiente e giusto. Guida alla lettura della riforma Cartabia (profili processuali)*, in "Sistema penale", novembre 2022
- M. GIALUZ (2020), *Premessa*, in "Diritto di internet", 2020, n. 3, suppl. (*Le nuove intercettazioni. Legge 28 febbraio 2020 n. 7*)
- M. GIALUZ, J. DELLA TORRE (2022), *Giustizia per nessuno. L'inefficienza del sistema penale italiano tra crisi cronica e riforma Cartabia*, Giappichelli, 2022
- M. GIALUZ, J. DELLA TORRE (2020), *Il progetto governativo di riforma della giustizia penale approda alla Camera: per avere processi rapidi (e giusti) serve un cambio di passo*, in "Sistema penale", aprile 2020
- L. GIORDANO (2022), *L'istituzione di un processo penale telematico*, in A. Basi, C. Parodi (a cura di), "La riforma del sistema penale", Giuffrè, 2022
- L. GIORDANO (2021), *La giurisprudenza di legittimità sulle prime applicazioni del processo penale telematico*, in "Sistema penale", maggio 2021
- L. GIORDANO (2020-A), *Disegno di legge delega per l'efficienza del processo penale: disposizioni su deposito telematico degli atti e notificazioni*, in "Il Processo Telematico", 2020
- L. GIORDANO (2020-B), *Il processo penale a distanza ai tempi del coronavirus*, in "Diritto penale e processo", 2020, n. 7
- L. GIORDANO (2019), *Impugnazioni cautelari. L'inserimento degli atti del procedimento nel sistema Tiap lede il diritto di difesa?*, in "il Penalista", 2019
- L. GIORDANO (2018), *Il sistema documentale Tiap: esame delle questioni sorte a qualche anno dalla sua introduzione*, in "il Penalista", 2018

- M. GRIFFO (2019), *Il captatore informatico e la filosofia del doppio binario*, Editoriale Scientifica, 2019
- F. IANNONE (2024), *APP non funziona! Cronaca di una difficile transizione digitale*, in “Giustizia insieme”, febbraio 2024
- E.N. LA ROCCA (2021), *Il modello di riforma “Cartabia”: ragioni e prospettive della Delega n. 134/2021*, in “Archivio penale web”, 2021, n. 3
- E.N. LA ROCCA (2019), *Notificazioni via PEC: i limiti di validità negli approdi della giurisprudenza penale*, in “Il Quotidiano giuridico”, giugno 2019
- G. LASAGNI (2023), *The Impact of Digital Technology on Italian Criminal Proceedings*, in “Zeitschrift für die gesamte Strafrechtswissenschaft”, 2023, n. 3
- G. LASAGNI (2016), *L'uso di captatori informatici (trojans) nelle intercettazioni “fra presenti”*, in “Diritto penale contemporaneo”, ottobre 2016
- R. LOPEZ (2022), *Nuove ipotesi di documentazione mediante videoregistrazione e collegamento a distanza*, in “Processo penale e giustizia”, 2022, n. 1
- S. LORUSSO (2020), *Il cigno nero del processo penale*, in “Sistema penale”, maggio 2020
- S. LORUSSO (2017), *Dibattimento a distanza vs. “autodifesa”?*, in “Diritto penale contemporaneo – Rivista Trimestrale”, 4, 2017, n. 4
- A. MADDALENA (2019), *Profili organizzativi del TIAP, esperienza del distretto di Napoli*, in A. Ciriello (a cura di), “Il processo telematico”, Key editore, 2019
- A. MALACARNE (2024), *Canone di concentrazione e calendario delle udienze*, in T. Bene, M. Bontempelli, L. Luparia Donati (a cura di), “Il procedimento penale tra efficienza, digitalizzazione e garanzie partecipative”, vol. II, in G.L. Gatta, M. Gialuz, “Riforma Cartabia. Le modifiche al sistema penale”, Giappichelli, 2024
- E.M. MANCUSO (2020), *La dematerializzazione del processo al tempo del COVID-19*, in “Giurisprudenza Penale Web”, 2020, n. 5
- S. MARCOLINI (2015), *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in “Cassazione penale”, 2015, n. 2
- O. MAZZA (2020), *Distopia del processo a distanza*, in “Archivio penale web”, 2020, n. 1
- M. MENNA, M. MINAFRA (2017), *Il dibattito: esame a distanza e restyling strutturale della sentenza*, in A. Scalfati (a cura di), “La riforma della giustizia penale. Commento alla legge 23 giugno 2017, n. 103”, Giappichelli, 2017
- M. MIRAGLIA (2024), *L'Ufficio per il processo*, in M. Caianiello, M. Gialuz, S. Quattrocchio (a cura di), “Il procedimento penale tra efficienza, digitalizzazione e garanzie partecipative”, vol. I, in G.L. Gatta, M. Gialuz, “Riforma Cartabia. Le modifiche al sistema penale”, Giappichelli, 2024
- M. MIRAGLIA (2023), *Il “Trojan (non) di Stato”: una disciplina da completare*, in “Processo penale e giustizia”, 2023, n. 5
- S. NAPOLITANO (2020), *Dall'udienza penale a distanza all'aula virtuale*, in “Sistema penale”, luglio 2020
- V. NARDO (2023), *La progressiva digitalizzazione del processo*, in “Processo penale e giustizia”, 2023, n. straordinario
- D. NEGRI (2023), *Atti e udienze “a distanza”: risvolti inquisitori di una transizione maldestra alla giustizia digitale*, in D. Castronuovo, M. Donini, E.M. Mancuso, G. Varraso (a cura di), “Riforma Cartabia. La nuova giustizia penale”, Cedam, 2023

- D. NEGRI (2018), *La gigantesca espansione della videoconferenza come alternativa alla presenza fisica dell'imputato in giudizio*, in "Archivio penale", 2018, n. speciale
- F. NICOLICCHIA (2023), *Domicilio digitale e notificazioni*, in D. Castronuovo, M. Donini, E.M. Mancuso, G. Varraso (a cura di), "Riforma Cartabia. La nuova giustizia penale", Cedam, 2023
- F. NICOLICCHIA (2020), *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Cedam, 2020
- W. NOCERINO (2021), *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Cedam, 2021
- R. ORLANDI (2014), *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in "Rivista italiana di diritto e procedura penale", 2014, n. 3
- L. PALMIERI (2023), *Le innovazioni digitali nel processo penale: tutto si agita e niente si muove*, in "PenaleDP", dicembre 2023
- L. PETRUCCI (2015), *Il tormentato avvio delle notifiche telematiche nel processo penale*, in "Questione giustizia", gennaio 2015
- F. PORCU (2022), *Digitalizzazione degli atti, videoriprese e partecipazione a distanza*, in G. Spangher (a cura di), "La riforma Cartabia", Pacini Editore, 2022
- P. RIVELLO (2017), *La disciplina della partecipazione a distanza al procedimento penale alla luce delle modifiche apportate dalla Riforma Orlando*, in "Diritto penale contemporaneo", 2017, n. 7-8
- F. RUGGIERI (2020), *Il processo penale al tempo del Covid-19: modelli alternativi di gestione della crisi*, in "La legislazione penale", maggio 2020
- G. SAVIO (2024), *APP, cronaca necessaria di un annunciato ma utile flop*, in "Questione giustizia", gennaio 2024
- S. SIGNORATO (2024), *Il processo penale telematico: alla ricerca di un punto di equilibrio tra efficienza e salvaguardia dei diritti fondamentali*, in "Rivista di diritto processuale", 2024, n. 2
- S. SIGNORATO (2023), *La gestione telematica dell'atto processuale nel dedalo del processo penale telematico*, in E.M. Catalano, R.E. Kostoris, R. Orlandi (a cura di), "Commenti alla legge n. 134 del 2021 e ai decreti legislativi delegati", vol. II, Riassetto della penality, razionalizzazione del procedimento di primo grado, giustizia riparativa, Giappichelli, 2023
- S. SIGNORATO (2017), *L'ampliamento dei casi di partecipazione a distanza dell'imputato tra logiche efficientistiche e menomazioni difensive*, in "Legislazione penale web", novembre 2017
- S. SIGNORATO (2012), *La localizzazione satellitare nel sistema degli atti investigativi*, in "Rivista italiana di diritto e procedura penale", 2012, n. 2
- G. SPANGHER (2021), *La riforma Cartabia nel labirinto della politica*, in "Diritto penale e processo", 2021, n. 9
- R. SUSSKIND (2019), *Online Courts and The Future of Justice*, Oxford University Press, 2019
- L. TAVASSI (2024), *Formalismi giurisprudenziali e forme tecnologiche nel giusto processo digitale*, in "Archivio penale web", 2024, n. 1
- P. TONINI (2022), *Le nuove tecnologie e la riforma Cartabia*, in "Diritto penale e processo", 2022, n. 3
- M. TORRE (2017), *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Giuffrè, 2017
- C. TRABACE (2023), *Il deposito telematico delle impugnazioni, prima, durante e dopo l'emergenza epidemiologica*, in "Archivio penale web", 2023, n. 1

- F. TRAPELLA (2022), *La rivoluzione digitale alla prova della riforma*, in “Archivio penale web”, 2022, n. 3
- N. TRIGGIANI (2020), *La partecipazione a distanza*, in E. Mezzetti, L. Luparia (diretto da), *La legislazione antimafia*, Zanichelli, 2020
- N. TRIGGIANI (2019), *Le videoriprese investigative e l'uso dei droni*, in A. Scalfati (a cura di), “Le indagini atipiche”, Giappichelli, 2019
- D. TRIPICCIONE (2022), *Atti e udienze a distanza*, in A. Bassi, C. Parodi (a cura di), “La riforma del sistema penale”, Giuffrè, 2022



SIMONE CAFIERO

Diritto di difesa, accesso a Internet e rimozione degli “ostacoli di ordine economico e sociale”

Muovendo da una ricostruzione del principio di eguaglianza sostanziale come principio che impone la rimozione delle disuguaglianze che attengono alla distribuzione delle “utilità fondamentali”, a ciascuna delle quali corrisponde la previsione di un diritto sociale costituzionalmente garantito, il presente lavoro si misura con il tema della costituzionalizzazione espressa di un diritto all’accesso alla Rete, in un contesto nel quale la possibilità di accedere efficacemente al cyberspazio rappresenta una condizione necessaria al pieno esercizio di un ampio insieme di diritti costituzionali. Un insieme, questo, che oggi – all’esito delle “riforme Cartabia” del processo civile e di quello penale – tende a includere anche il diritto di azione e quello di difesa.

Eguaglianza – Utilità fondamentali – Accesso alla rete – Diritto di difesa

Right of defense, Internet access and the removal of social and economic obstacles

By construing the principle of substantial equality as a principle entailing the removal of those inequalities which pertain to the distribution of the so-called “fundamental resources”, each of which corresponds to the constitutional provision of a specific social right, the paper tackles the issue of the explicit constitutionalization of a right to access the Net, in a context in which an adequate access to the cyberspace constitutes a necessary condition for the full enjoyment of a considerable number of rights. Today, as a consequence of the “Cartabia reforms” of civil and criminal procedural law, such rights also include the right of action and the right of defense.

Equality – Fundamental resources – Access to the Net – Right of defense

L’Autore è assegnista di ricerca in Diritto costituzionale presso l’Università degli Studi di Napoli Federico II

Questo lavoro è stato parzialmente finanziato dal progetto NextGenerationEU “Security and Rights in CyberSpace” (SERICS) e dal progetto NextGenerationEU “Digitalization of the judiciary functions: trends, perspectives and risks” (PRIN PNRR, Codice progetto: P2022PRBCS, CUP D53D23022420001)

Questo contributo fa parte della sezione monografica *Digitalizzazione del processo e diritti fondamentali – Profili processuali* a cura di Francesca Bailo e Michele Francaviglia

SOMMARIO: 1. Introduzione. – 2. Eguaglianza sostanziale e utilità fondamentali. – 3. L'accesso alla rete come utilità fondamentale disegualmente distribuita. – 4. Il diritto (sociale) all'accesso alla rete: dall'art. 21-*bis* all'art. 34-*bis* Cost. (e ritorno).

1. Introduzione

Muovendo dalla relazione svolta in occasione del seminario *Process Digitalization and Fundamental Rights*, tenutosi presso l'Università degli Studi di Genova il 9 maggio 2024, il presente scritto intende proporre una riflessione in qualche misura preliminare alle altre presentate in occasione di tale giornata di studi. A giudizio di chi scrive, molti dei temi emersi nel corso del seminario, specie in merito all'evoluzione telematica del processo, impongono di soffermare l'attenzione sul rilievo costituzionale dell'accesso alla rete come risorsa indispensabile, oggi, per l'esercizio di un ampio insieme di diritti costituzionali; un insieme cui vanno progressivamente aggiungendosi – per tutte le ragioni ampiamente illustrate dagli intervenuti – anche i diritti di azione e di difesa, sol che si tenga presente l'intrinseco legame di questi ultimi con la configurazione strutturale del processo¹. Nello specifico, la consapevolezza di questi fenomeni rende utile tornare a interrogarsi sull'opportunità,

o meno, di una positivizzazione costituzionale del diritto di accesso alla rete, così come sulle connotazioni da imprimere, eventualmente attraverso espresse previsioni costituzionali, a questo diritto. È con queste questioni che il presente lavoro intende misurarsi, muovendo da una specifica interpretazione del principio di eguaglianza sostanziale che a chi scrive sembra, fra tutte quelle proposte dalla dottrina, la più convincente.

2. Eguaglianza sostanziale e utilità fondamentali

Che l'art. 3, co. 2, Cost. rappresenti una delle disposizioni più innovative e politicamente connotate – e già sol per questo giuridicamente più dibattute – dell'intero testo costituzionale è valutazione condivisa in dottrina². Altrettanto condivisa è la valutazione circa la prima e fondamentale indicazione di senso che deve trarsi, quanto ai rapporti tra Stato e società civile, dalla medesima disposizione: come che si voglia interpretarla, essa impone al potere pubblico di non disinteressarsi dell'assetto

1. Concetto, questo, che la dottrina penalistica esprime scorrendo di “relatività” del diritto di difesa. Sul punto si veda VOENA 1988, p. 12: «il contenuto del diritto di difesa non può che porsi in relazione ad un assetto processuale alla cui edificazione esso non concorre in maniera diretta». In argomento, più di recente, anche PANSINI 2019. Pur senza ricorrere alla formula della “relatività”, la giurisprudenza costituzionale sembra condividere un simile approdo: sin dalla sent. n. 46/1957 la Corte costituzionale ha affermato che rientra nella discrezionalità del legislatore delineare più tipi di procedimento e che, laddove ciò avvenga, il diritto di difesa si adatta ai caratteri e agli scopi di ciascuno di essi, purché ciò non comporti la sostanziale vanificazione del diritto stesso; linea, questa, poi confermata da un'ampia giurisprudenza successiva, nell'ambito della quale è possibile ricordare almeno le sentt. nn. 62/1971, 46/1975, 162/1975 e 174/1976. Per considerazioni generali sul diritto di difesa e su quello di azione, senza pretesa di esaustività, si rinvia altresì a SATTA 1959, p. 822 ss.; BELLAVISTA 1964, pp. 454 ss.; COMOGGIO 1981, pp. 1-81; SCAPARONE 1981, pp. 82-118; GOLDONI-REALI 1988; VOENA 1988; FERRUA 1989; POLICE 2008, *passim*.

2. Sul punto, per tutti, FERRARA 1978, p. 89; PIZZORUSSO 1983, p. 49; SORRENTINO 2011, p. 10.

complessivo dei rapporti in cui la società civile si struttura, dovendo anzi intervenire su questi ultimi per assicurare il conseguimento di risultati che le spontanee – ma di certo non “naturali” – dinamiche della società civile medesima, lasciate a se stesse, non sono in grado di garantire³. È invece sulla misura di tale intervento – su ciò che lo Stato è autorizzato o tenuto a fare nell'esercizio delle funzioni ad esso connesse – che si è registrato, nel corso del tempo, il più ampio ed aspro dibattito dottrinale.

Vi sono state, sul punto, tesi “massimaliste” che nel principio di eguaglianza sostanziale hanno letto l'obbligo costituzionale del superamento dell'assetto capitalistico e della costruzione, attraverso una trasformazione «totale» dei rapporti economici, di una società tendenzialmente priva di diseguaglianze⁴: in un caso, tale linea interpretativa ha consentito – previa la costruzione delle norme costituzionali a garanzia della proprietà e dell'iniziativa economica privata come «norme temporanee» – di argomentare la realizzabilità, a Costituzione vigente, di un sistema socialista, improntato al *minimum* del controllo pubblico dell'attività economica e del superamento della divisione della società in classi⁵.

Vi sono state, al contrario, tesi “moderate” che, muovendo proprio dalla tutela costituzionale della proprietà e dell'iniziativa economica, nonché talvolta dal più discutibile assunto di un rilievo costituzionale generale del merito personale, hanno interpretato l'eguaglianza sostanziale in piena continuità e coerenza con il sistema capitalistico esistente, sostenendo che il principio in discorso si limiterebbe ad esprimere esigenze di semplice *adeguamento* – e perciò stesso di *conservazione* – di esso, prescrivendo unicamente la rimozione di quelle diseguaglianze che più manifestamente

incidono sulle possibilità di realizzazione individuale e di partecipazione alla competizione per le risorse e le posizioni sociali⁶.

Non sono mancate neppure tesi marcatamente svalutative del principio in esame, protese in realtà a negarne la rilevanza come principio autonomo, talvolta riducendolo a disposizione meramente riassuntiva delle singole «promesse» di intervento pubblico a sollievo di specifiche situazioni di bisogno previste dalla Costituzione, talvolta attribuendovi il valore «servente» di semplice garanzia dell'eguaglianza formale⁷.

Un utile punto di orientamento per superare l'*impasse* è offerto da quelle proposte che, collocandosi su un piano diverso rispetto a quelle ora accennate, attraverso una lettura analitica dell'art. 3, co. 2, Cost. operano una distinzione tra la «rimozione degli ostacoli di ordine economico e sociale» che incidono di fatto sulla libertà e l'eguaglianza dei cittadini, da un lato, e il «pieno sviluppo della persona umana» e la «effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese», dall'altro. In questa chiave, nel pieno sviluppo della persona e nell'effettiva partecipazione dei lavoratori si collegano i fini ultimi della disposizione, da realizzare attraverso il superamento del modello di società diseguale che era sotto gli occhi dei costituenti e la costruzione, attraverso l'opera dei pubblici poteri e in primo luogo del legislatore, di un modello di società alternativo. Tuttavia, poiché la Costituzione non predetermina i caratteri del modello di società da instaurare, limitandosi a stabilire che debba trattarsi di una società in cui siano assicurati il pieno sviluppo della persona e l'effettiva partecipazione dei lavoratori, è al legislatore – e quindi alle forze politiche e sociali che ne animano e ne

3. Così, in termini generali, MORTATI 1975, p. 9, nonché PIZZORUSSO 1987, p. 1057. Sul punto si veda anche GIANINI 1979, pp. 391-394.

4. Di «cambiamento di segno della *totalità*» parla ROMAGNOLI 1975, p. 168. Nello stesso senso sembrano doversi intendere le considerazioni di FICHERA 1974, spec. pp. 33 e 39.

5. È la tesi, molto nota e molto criticata, di LAVAGNA 1977, pp. 28-30 e 67 ss.

6. Questa lettura, che può oggi considerarsi maggioritaria, si riscontra, fra gli altri, in CERRI 1984, p. 139; PIZZORUSSO 1993 (e per la posizione dell'autore si veda anche PIZZORUSSO 1983, p. 52); D'ALOIA 2002, pp. 65 e 77-85; CATTANEO 1999, pp. 6 e 9; CAMERLENGO 2013, p. 69 ss.

7. Nel primo senso ESPOSITO 1954, p. 61; nel secondo ROSSANO 2005, p. 443 (e per la posizione dell'autore si veda anche ROSSANO 2006, pp. 2156-2157), nonché DI GASPARE 2008.

stimolano l'operato – che spetta delineare il «progetto di trasformazione» in cui tali scopi si concretizzano⁸. Insomma, il significato delle locuzioni «pieno sviluppo della persona umana» ed «effettiva partecipazione dei lavoratori» *non è giuridicamente predeterminato*, neppure dalla Costituzione, giacché «queste finalità si riempiono di contenuto nel gioco dei rapporti sociali»⁹. Se ne ricava una conseguenza di rilievo: la sufficienza o meno, l'adeguatezza o meno del disegno di trasformazione sociale attraverso cui si perseguono tali finalità non è sindacabile dalla Corte costituzionale, e ciò non già perché esse siano definite attraverso clausole «elastiche», ma perché la loro formulazione nel testo costituzionale ne rinvia la concretizzazione a determinanti politiche a cui – innanzitutto per le forme della sua legittimazione – il giudice delle leggi deve mantenersi estraneo¹⁰.

Tutto ciò non significa che l'art. 3, co. 2, Cost. sia privo di contenuti giuridicamente vincolanti. Innanzitutto, giuridicamente doveroso è in sé il perseguimento degli scopi del «pieno sviluppo della persona» e dell'«effettiva partecipazione di tutti i lavoratori», qualunque sia il significato che concretamente le forze politiche scelgano di attribuire a tali formule; dal che dovrebbe trarsi che un «progetto di trasformazione sociale», quale che esso sia, è necessario, restando esclusa dal novero delle potenziali condotte attuative dell'articolo in questione la mera presa d'atto delle disuguaglianze che connotano il modello di società esistente. E sebbene, per le ragioni dette, ciò non consenta alcun intervento «sostitutivo» alla Corte costituzionale, cionondimeno la precisazione appare necessaria ad intendere pienamente il senso complessivo della disposizione in esame.

In secondo luogo, e soprattutto, giuridicamente doveroso è il «mezzo» della trasformazione sociale, rappresentato dalla «rimozione degli ostacoli di ordine economico e sociale» che *di fatto* – vale a dire nel concreto atteggiarsi delle dinamiche effettive della società – limitano la libertà e l'eguaglianza fra i cittadini astrattamente proclamate dal diritto¹¹. In altre parole, quali che siano gli scopi perseguiti dalle forze politiche *sub specie* di «pieno sviluppo della persona» ed «effettiva partecipazione di tutti i lavoratori», lo strumento per perseguirli è costituzionalmente vincolato, ed è rappresentato dalla rimozione delle disuguaglianze che, prodotte dal concreto assetto della società, incidono sulla libertà e l'eguaglianza dei cittadini nel pieno esercizio dei diritti. Sul punto, di estrema utilità appare la formula con cui, ben prima del suo formale inserimento nel nuovo testo costituzionale in corso di approvazione, Giannini prefigurava il principio in parola: «un principio generale il quale dica che spetta all'azione dello Stato eliminare le disuguaglianze che si producono nella collettività e che siano imputabili a fatti attinenti al corpo sociale stesso»¹². Secondo una lettura che è stata fatta propria tra i costituzionalisti da Barbara Pezzini e Andrea Giorgis, e fra i filosofi del diritto da Nicola Riva, la «rimozione degli ostacoli di ordine economico e sociale» consiste precisamente nella *rimozione delle disuguaglianze che riguardano l'accesso alle utilità/opportunità fondamentali*, e cioè alle risorse (materiali o immateriali) necessarie al pieno ed effettivo esercizio dei diritti.

L'interpretazione del principio di eguaglianza sostanziale qui accolta ha il pregio di ricavare dall'art. 3, co. 2, Cost. un apprezzabile significato giuridico, senza per questo tacerne le valenze più

8. La più compiuta formulazione di questa proposta interpretativa si riscontra in CARAVITA 1984, p. 58 ss. (per il concetto di «progetto di trasformazione», invero fondamentale nella ricostruzione compiuta dall'autore, cfr. pp. 86-87). Essa si trova condivisa in RESCIGNO 1999, p. 120-121. Un'anticipazione di questa lettura può trovarsi in Atripaldi 1974, p. 12: «Se poi la individuazione del modello di società da instaurare può sembrare embrionale e allusiva, ciò si spiega con il fatto che l'intenzione del Costituente era quella di disegnare un modello dinamico di società per la cui realizzazione si è considerata essenziale la rimozione degli ostacoli di ordine economico e sociale, lasciando la rilevazione concreta e definitiva di questi ad una valutazione storica». Sul carattere dinamico, aperto a più soluzioni, del «percorso» indicato dall'art. 3, co. 2, Cost. si veda anche LUCIANI 1995, p. 146.

9. CARAVITA 1984, p. 91.

10. *Ivi*, pp. 91-93. Nel medesimo senso sembrano doversi intendere le considerazioni di RESCIGNO 1999, pp. 123-124.

11. CARAVITA 1984, pp. 65-75. Nello stesso senso si veda anche ANDREONI 2006, spec. p. 92 ss.

12. GIANNINI 2016, p. 25.

schiettamente politiche. Un delicato equilibrio, questo, che sembra sfuggire alle altre proposte interpretative sopra accennate. In effetti, il limite delle teorie “massimaliste” sta nel sottovalutare il carattere «estroverso» rispetto all’ordinamento¹³, di rinvio agli orientamenti dei partiti politici e delle forze sociali concrete, della formulazione dell’art. 3, co. 2, Cost., dando per già configurato quello che spetta solo a queste ultime configurare, ossia il modello di società – comunque diverso da quello esistente – attraverso la cui costruzione realizzare il «pieno sviluppo della persona umana» e la «effettiva partecipazione dei lavoratori». Di contro, il torto delle teorie “moderate” sta nell’amputare una parte della disposizione, leggendo l’art. 3, co. 2, come se si limitasse a imporre la rimozione degli ostacoli che di fatto incidono sul libero e uguale esercizio dei diritti, senza fare alcuna menzione dei fini ulteriori del «pieno sviluppo» e della «effettiva partecipazione», la cui realizzazione implica comunque lo sforzo di prefigurare e di perseguire un modello di società diverso da quello esistente.

È precisamente a questo punto del discorso sull’eguaglianza sostanziale che si inseriscono i diritti sociali: senza esaurire il contenuto del principio, questi diritti rappresentano una prima concretizzazione, discendente direttamente dal testo della Costituzione, del compito di rimozione degli ostacoli che in forza di esso grava sull’insieme dei poteri pubblici¹⁴. Nelle parole di Crisafulli, scopo di questi diritti è *incidere sull’organizzazione economica della società civile*¹⁵, con il fine di *sottrarre all’allocazione attraverso il mercato* – e quindi alle diseguaglianze che ne deriverebbero – le *utilità ritenute fondamentali* affinché il soggetto possa

ritenersi libero ed eguale agli altri nel pieno esercizio dei diritti attribuitigli dall’ordinamento¹⁶. Insomma, secondo questa interpretazione, sottesa ad ogni diritto sociale vi è la consapevolezza di un’utilità fondamentale che, nelle concrete dinamiche della società civile, tende ad essere disegualmente distribuita: un lavoro dal quale ricavare il proprio sostentamento, una retribuzione sufficiente a consentire una vita libera e dignitosa, un buono stato di salute psicofisica, un adeguato livello di istruzione e così via.

3. L’accesso alla rete come utilità fondamentale disegualmente distribuita

Che la possibilità di accedere efficacemente alla rete rappresenti una risorsa disegualmente distribuita sembra adeguatamente dimostrato dalla copiosa letteratura, non solo scientifica, fiorita intorno alle varie manifestazioni del fenomeno del *digital divide*. Formula, questa, con la quale si indica il «perdurante discriminare (dovuto a fattori culturali, economici e generazionali) tra una parte della popolazione, in grado di sfruttare, almeno parzialmente, le potenzialità offerte dalla rete, ed un’altra parte, che rimane priva degli strumenti per accedervi ed ivi esercitare i diritti e le libertà previste dall’ordinamento, nonché ad adempiere i doveri che – in modo crescente – non possono prescindere dall’utilizzo dello strumento informatico»¹⁷. Una simile definizione – merita osservarlo per inciso – chiarisce come i fattori produttivi di tale divario non siano solo quelli geografici, legati alla maggiore o minore copertura di segnale che caratterizza le diverse aree del territorio nazionale:

13. Sul quale nuovamente CARAVITA 1984, pp. 83-84.

14. *Ivi*, p. 89.

15. Per questa formula, invero fondamentale nel discorso che si va svolgendo, si veda CRISAFULLI 1954, p. 73.

16. In tal senso BARCELLONA 1994, p. 327, ove i diritti in questione vengono appunto descritti come «diritti fondamentali che comportano una distribuzione di risorse fuori mercato». Sulla stessa linea PEZZINI 2001, p. 189, secondo cui si è in presenza di diritti sociali laddove vi siano «disposizioni costituzionali che prescrivono, in termini di doverosità, la protezione degli interessi relativi al conseguimento ed al godimento di beni essenziali per la vita degli individui». Nello stesso senso, di «allocazione egualitaria di alcuni beni, sì da rendere possibile a ciascun individuo il pieno sviluppo della propria personalità e l’effettiva partecipazione all’organizzazione politica, economica e sociale del Paese» discorre GIORGIS 1999, p. 6.

17. NANNIPIERI 2013, p. 3. In argomento, senza pretesa di esaustività, si vedano anche DE MINICO 2009, spec. p. 552 ss.; RODOTÀ 2014, spec. p. 359; TANZARELLA 2013, p. 520-521; LOTTA 2020, p. 61 ss.; BUZZACCHI 2020, *passim*; ZUDDAS 2020, p. 285 ss.; CLARONI 2021, p. 215 ss.

a tali elementi, di per sé estremamente significativi, si aggiungono ragioni di ordine economico e, ancora, ragioni di ordine culturale, che hanno a che fare con i diversi livelli di alfabetizzazione informatica degli individui¹⁸. Dall'insieme di questi fattori risulta un quadro complessivo nel quale solo una parte della popolazione è posta nelle condizioni di accedere efficacemente alla rete. Un divario, questo, che si presta ad essere misurato in cifre: un rapido sguardo al rapporto DESI (*Digital Economy and Society Index*) 2022 rivela che, in Italia, la percentuale delle famiglie che possono avvalersi della banda larga fissa è pari al 66%, contro il 78% della media europea, mentre la percentuale delle famiglie raggiunte dalla rete fissa ad altissima capacità (VHCN) si attesta appena al 44%, contro il 70% della media europea. Secondo la medesima indagine, ancora, solo il 46% della popolazione italiana è in possesso delle competenze digitali di base, percentuale che scende al 23% ove si considerino le competenze superiori a quelle basilari. Del resto, è proprio muovendo da simili dati – il riferimento è, in particolare, al DESI 2020, che recava risultati ancor più negativi di quelli certificati dal DESI 2022, collocando l'Italia al ventiquattresimo posto tra i 27 Stati membri dell'Ue – che il Pnrr fa della «digitalizzazione» la prima delle sue sei «missioni», ricomprendendovi interventi volti non solo ad incrementare la disponibilità di reti fisse e mobili ad altissima capacità, ma anche a colmare i divari fra i cittadini sul piano delle conoscenze e competenze digitali¹⁹.

Eppure, che un accesso alla rete efficace – sul piano degli strumenti e delle competenze – rappresenti oggi una risorsa indispensabile per il

pieno ed effettivo esercizio dei diritti previsti dalla Costituzione è ormai pacificamente ammesso dalla dottrina. In questa chiave, si è evidenziato che «oggi, nella società dell'informazione o, se si preferisce, nell'era dell'accesso [...], non avere accesso a Internet significa vedersi precluso l'esercizio della più parte dei diritti di cittadinanza», anche perché «sempre di più l'accesso alla rete Internet, e lo svolgimento su di essa di attività, costituisce il modo con il quale il soggetto si relaziona con i pubblici poteri»²⁰. Da una prospettiva complementare, si è osservato che «i vantaggi della connessione veloce sono [...] valutabili in termini di inclusione della persona nel processo sociale e politico», in quanto «l'accesso veloce [...] agendo da leva atta a sollevare gli ostacoli materiali ed economici al pieno sviluppo della persona, diventa l'occasione per l'effettivo esercizio delle libertà fondamentali – manifestazione del pensiero, comunicazione intersoggettiva – alle quali taluni, gravati dalle preoccupazioni del vivere quotidiano (art. 2 Cost.) sono spesso costretti a rinunciare»²¹. Nella stessa chiave l'art. 2, co. 1, della Dichiarazione dei diritti di Internet – atto di indirizzo adottato nel luglio 2015 dalla Commissione per i diritti e i doveri relativi ad Internet istituita presso la Camera dei deputati – qualifica l'accesso ad Internet come «condizione per il [...] pieno sviluppo individuale e sociale» della persona²².

Ebbene, una simile conclusione risulta ulteriormente suffragata proprio dalla prospettiva di una svolta in senso digitale della disciplina del processo, svolta che – come pure si è detto nel corso del seminario – compie alcuni passi significativi proprio con le due cd. «riforme Cartabia»: quella del processo civile, avviata con la delega legislativa

18. In tal senso ALLEGRI 2021, p. 59; D'IPPOLITO 2021, p. 96.

19. Sul punto MONTAGNANI 2022.

20. FROSINI 2011, pp. 10 e 8. Nello stesso senso si veda RODOTÀ 2012, pp. 387-388, ove la considerazione delle peculiarità della rete, quanto alla «definizione/costruzione» di «quel complessivo patrimonio di diritti» in cui si sostanzia la cittadinanza, conduce l'autore ad affermare che «essere esclusi da questo circuito incide direttamente sull'esercizio dei diritti». Considerazioni analoghe, *ex multis*, in TANZARELLA 2013, p. 517; ALLEGRI 2016, p. 8; TANZARELLA 2021, pp. 40-42; DE RADA 2023, pp. 5-7.

21. DE MINICO 2011, par. 1. Per il pensiero dell'autrice si veda anche DE MINICO 2016, pp. 3-4, ove si osserva che «se la rete è essenziale per compiere la dimensione costituzionale della persona, e qui Internet rileva come patrimonio aperto da cui ciascuno attinge conoscenza per accelerare la propria inclusione nel processo politico-democratico, essa diventa un bene indispensabile, non diversamente dai diritti fondamentali esercitati per suo tramite».

22. L'importanza di questa parte della disposizione è segnalata, fra gli altri, da BUSACCA 2017, spec. pp. 345-347.

conferita al Governo dalla l. n. 206/2021 e portata a compimento con il conseguente d.lgs. n. 149/2022; e quella del processo penale, sviluppatasi attraverso la delega legislativa di cui alla l. n. 134/2021, il connesso d.lgs. n. 150/2022 e – da ultimo – il decreto del Ministro della giustizia n. 217/2023.

Quanto alla “riforma Cartabia” del processo civile²³, nella prospettiva che qui interessa le innovazioni più rilevanti sono due. Da un lato c'è la generalizzazione dell'impiego dello strumento telematico, ed in specie della posta elettronica certificata, per i depositi, le notifiche e le comunicazioni, compiuta dal d.lgs. n. 149/2022 introducendo il nuovo art. 149-*bis* c.p.c. e modificando la l. n. 53/1994 e il d.l. n. 179/2012; un'innovazione che ha raccolto ampi consensi in dottrina, per le sue obiettive virtù semplificatorie. Dall'altro lato c'è la previsione, a norma del nuovo co. 3 dell'art. 127, che il giudice possa disporre lo svolgimento dell'udienza mediante collegamento audiovisivo o la sua sostituzione con il deposito di note scritte. Merita osservare che entrambe le ipotesi di gestione alternativa dell'udienza sono previste *in via generale*: a norma dei successivi artt. 127-*bis* e 127-*ter* c.p.c., esse possono applicarsi a tutte le udienze che non richiedano «la presenza di soggetti diversi dai difensori, dalle parti, dal pubblico ministero e dagli ausiliari del giudice».

Quanto alla “riforma Cartabia” del processo penale²⁴, ampio consenso dottrinale hanno riscosso il principio generale della redazione degli atti scritti in forma di documento informatico, posto dal nuovo testo dell'art. 110 c.p.p.; la generalizzazione del deposito in via telematica di atti e

documenti, a norma del nuovo art. 111-*bis* c.p.p.; la previsione, ad opera del nuovo art. 111-*ter* c.p.p., di un fascicolo telematico tendenzialmente esaustivo, che raccoglie gli atti e i documenti creati *ab origine* in formato informatico, quelli depositati in formato analogico e successivamente convertiti dall'ufficio in documenti informatici e un elenco di quelli depositati in formato analogico e non suscettibili di digitalizzazione. Per converso, le principali riflessioni critiche hanno riguardato gli artt. 133-*bis* e 133-*ter* c.p.p., anch'essi introdotti dalla riforma. Trattasi di disposizioni che consentono all'autorità giudiziaria di stabilire che un determinato atto sia compiuto a distanza, oppure che una o più parti possano partecipare a distanza al compimento di un atto o alla celebrazione di un'udienza, mediante collegamento audiovisivo.

Ci si avvede che, con la parziale eccezione dei nuovi artt. 133-*bis* e 133-*ter* c.p.p., le innovazioni recate dalle due «riforme Cartabia» presuppongono l'accesso alla rete non tanto ad opera della parte, quanto piuttosto ad opera del suo difensore: sarà questi, ad esempio, a doversi avvalere della posta elettronica certificata per depositare e notificare atti, a depositare – sempre in via telematica – le note scritte in sostituzione d'udienza di cui all'art. 127-*ter* c.p.c., a consultare il fascicolo telematico di cui all'art. 111-*ter* c.p.p. E tuttavia, poiché nella generalità dei casi il compimento degli atti di parte richiede l'assistenza tecnica di un difensore, la cui *ratio* si coglie nella «necessità di una completa e corretta prospettazione, in termini giuridici, delle ragioni e richieste delle parti necessaria nella generalità dei procedimenti giurisdizionali»²⁵, la

23. Per la riflessione dottrinale si vedano, *ex multis*, BIAVATI 2022, p. 45 ss.; PICCININNI 2023; POLI 2023. Per considerazioni (anche critiche) sulle soluzioni emergenziali adottate nel corso della pandemia da Covid-19, che anticipano alcuni dei caratteri della riforma, BIAVATI 2021, nonché BRONZINI 2021.

24. Senza pretesa di esaustività, si rinvia a RIZZUTO 2022; TONINI 2022; NARDO 2023; GALGANI 2023; DEI-CAS 2023.

25. POLICE 2008, pp. 19-20. Sul rapporto tra l'assistenza tecnica di un difensore e l'esercizio dei diritti di azione e di difesa si vedano anche BELLAVISTA 1964, pp. 457-461; FERRUA 1989, pp. 6-9; COMOGGIO 1981, pp. 53-60; GOLONI-REALI 1988, p. 1. Il nesso in questione è stato valorizzato anche dalla giurisprudenza costituzionale: in C. cost., sent. n. 178/1970, punto 2 del Considerato in diritto, si legge ad esempio che «[n]on è contestabile [...] che il diritto inviolabile alla difesa, garantito in ogni stato e grado del procedimento dall'art. 24, debba implicare l'effettiva assistenza tecnica e professionale, così da consentire alle parti di far valere, attraverso un regolare contraddittorio, le proprie ragioni». Il legame tra il diritto di difesa e l'assistenza tecnica prestata dal difensore, quale strumento per far valere nel processo le ragioni della parte, è affermato con ancor più forza nella già citata sent. n. 46/1957, nel cui Considerato in diritto si può leggere quanto segue: «[i]l diritto della difesa, pertanto, intimamente legato alla esplicazione del potere giurisdizionale e alla possibilità di rimuovere le difficoltà di carattere economico che possono opporsi (come si è detto nel terzo comma dello stesso art. 24) al concreto esercizio del

possibilità per il difensore di avvalersi, in ogni luogo del territorio nazionale, di un efficace accesso alla rete che gli consenta di svolgere le suddette attività incide direttamente sull'esercizio dei diritti di azione e di difesa della parte.

Insomma, nello scenario – che le due «riforme Cartabia» cominciano a delineare – di una progressiva digitalizzazione del processo, il diritto di difesa e anche quello di azione si aggiungeranno al novero dei diritti costituzionali il cui pieno esercizio può essere pregiudicato dalla diseguale distribuzione dell'accesso alla rete. Anche per tale ragione, dunque, quest'ultimo dovrà ascriversi al novero degli «ostacoli di ordine economico e sociale» di cui l'art. 3, co. 2, Cost. prescrive la rimozione.

A parere di chi scrive, le considerazioni fin qui svolte delineano un quadro di riferimento utile ad affrontare il problema, tutt'oggi aperto e discusso dalla dottrina, della positivizzazione in Costituzione di un diritto all'accesso alle reti telematiche²⁶. Non si tratta, con ogni evidenza, di un tema nuovo: dalla sua prima apparizione, che va rintracciata nella proposta formulata da Stefano Rodotà in occasione dell'*Internet Governance Forum* del 2010, esso ha attraversato diverse stagioni e dato luogo a una pluralità di reazioni, talvolta critiche, talvolta adesive.

L'idea di arricchire il «catalogo» dei diritti costituzionali con un diritto di accesso alla rete non ha mancato, invero, di suscitare obiezioni. Una prima obiezione è quella secondo cui la possibilità di accedere alla rete sarebbe già adeguatamente tutelata dal testo costituzionale vigente, non però come oggetto di un autonomo diritto, bensì in quanto mezzo per l'esercizio di taluni altri diritti costituzionali, e segnatamente della libertà di manifestazione del pensiero (art. 21 Cost.)²⁷. Allo stadio attuale del progresso tecnologico nel settore delle telecomunicazioni, la tutela costituzionale della suddetta situazione giuridica soggettiva includerebbe già oggi la pretesa ad accedere liberamente al «mezzo» telematico, quale veicolo della comunicazione fra soggetti e dell'espressione delle idee. Se ne ricava che, non meritando la rete alcuna considerazione privilegiata rispetto agli altri mezzi attraverso cui è possibile esercitare il diritto di cui all'art. 21 Cost., non vi sarebbe ragione di farne oggetto di una previsione costituzionale apposita²⁸.

A una simile ricostruzione potrebbe in primo luogo obiettarsi che, nelle sentt. nn. 105/1972 e 225/1974, la Corte costituzionale ha affermato che la tutela costituzionale della libertà di manifestazione del pensiero non comporta il diritto di tutti ad avere «la materiale disponibilità» di qualsiasi possibile mezzo di diffusione, bensì solo

diritto medesimo, deve essere inteso come potestà effettiva della assistenza tecnica e professionale nello svolgimento di qualsiasi processo, in modo che venga assicurato il contraddittorio e venga rimosso ogni ostacolo a far valere le ragioni delle parti». Nel passo appena citato, a ben vedere, la Corte sembra addirittura risolvere l'intero contenuto del «diritto della difesa» nella effettiva possibilità di avvalersi dell'assistenza tecnica di un difensore.

26. Questa formula (che in seguito si semplificherà, solo per brevità, in «diritto di accesso alla rete») risulta preferibile a quella – certamente più puntuale e di più immediata comprensione – di «diritto di accesso a Internet» per le ragioni illustrate da ALLEGRI 2016, p. 22: «Internet [...] non è un nome comune riferito genericamente alle reti telematiche interconnesse, ma è un *nome proprio* con il quale si indica l'infrastruttura reticolare più diffusa al mondo, che ha un'origine storica, delle specifiche caratteristiche fisiche e tecniche e soprattutto – per ciò che interessa principalmente il giurista – un proprio sistema di *governance* mediante specifici istituti (peraltro, almeno finora, di matrice statunitense). Internet è una sola fra le possibili reti telematiche, benché quella oggi di più vaste proporzioni, ed è solo la diffusione delle connessioni a Internet a livello planetario che ha determinato l'estensione di questo termine per antonomasia al concetto di «sistema di reti telematiche interconnesse» (corsivo nel testo).

27. Com'è noto, a consentire questa interpretazione è la formulazione particolarmente ampia dell'art. 21, co. 1, Cost., laddove si garantisce a tutti la libertà di manifestare il proprio pensiero «con la parola, lo scritto e ogni altro mezzo di diffusione».

28. In tal senso POGGI 2020; LOTTA 2020, pp. 67 ss.; ROSSETTI 2011, pp. 93-97. Pur muovendo dalla medesima ricostruzione, maggiormente favorevoli alla prospettiva di un'espressa positivizzazione si mostrano AZZARITI 2011, par. 4, e COSTANZO 2012, pp. 5-6.

la garanzia, ad opera della legge, della «giuridica possibilità di usarne o di accedervi»²⁹. Una conclusione, questa, che spezza quel legame tra titolarità della libertà di espressione e implicita garanzia del concreto accesso alla rete su cui si regge la tesi dianzi esaminata³⁰.

Anche a non condividere la linea argomentativa della Corte, poi, la tesi in esame risulta ugualmente poco persuasiva, per l'assorbente ragione che – come osservato *supra* – un efficace accesso al cyberspazio deve ormai considerarsi una precondizione indispensabile per il pieno esercizio di una pluralità di diritti costituzionali, che va molto al di là della sola libertà di manifestazione del pensiero: dalla libertà delle comunicazioni interpersonali alla libertà di iniziativa economica privata, dal diritto al lavoro al diritto all'istruzione passando per alcune declinazioni del diritto alla salute³¹, tendendo ad includere – oggi, all'esito delle due riforme Cartabia – persino i diritti di azione e di difesa. In tale contesto, a chi scrive pare vi siano solidi argomenti per affermare l'inadeguatezza di una tutela costituzionale solo «riflessa» dell'accesso alla rete, quale semplice risvolto o mera implicazione della libertà di espressione, ancorché considerata nelle sue molteplici declinazioni.

La seconda obiezione all'espressa costituzionalizzazione di un diritto di accesso alle reti si regge, a ben vedere, su argomenti opposti a quelli che sostengono la prima: si afferma infatti che un simile diritto non necessiterebbe di essere reso oggetto di una disposizione costituzionale espressa, perché potrebbe già oggi ritenersi un diritto sociale di rilievo costituzionale, ricavabile, sia pur per implicito, dall'art. 3, co. 2, Cost.³². A questa lettura può accostarsi quella di chi, rinunciando a parlare di un diritto sociale all'accesso a Internet, configura la promozione di un accesso efficace in tutte le aree

geografiche del paese (e presso tutti i gruppi sociali in cui esso si articola) come un compito oggettivo, un «servizio pubblico universale necessario per il godimento di diritti fondamentali costituzionalmente previsti» riconducibile, in quanto tale, al medesimo art. 3, co. 2, Cost.³³.

Anche ricostruzioni di questo genere non appaiono, perlomeno a chi scrive, in grado di revocare in dubbio l'utilità dell'adozione di una disposizione costituzionale espressa, che enunci con chiarezza un diritto sociale. Vero è che già oggi le azioni intraprese dal legislatore per diffondere e potenziare l'accesso alla rete possono trovare un loro fondamento costituzionale nell'opera di rimozione degli ostacoli di ordine economico e sociale prescritta dal principio di eguaglianza sostanziale. Tuttavia – secondo la proposta sistematica formulata *supra* – la logica complessiva sottesa al combinato disposto tra l'art. 3, co. 2, Cost. e le singole disposizioni costituzionali sui diritti sociali è quella secondo cui per ciascuna delle risorse, materiali o immateriali, più strettamente necessarie all'esercizio dei diritti costituzionali (le utilità fondamentali) l'ordinamento appresta uno specifico diritto sociale, volto a contrastarne la diseguale distribuzione per effetto delle spontanee dinamiche della società civile. Ebbene, in coerenza con quanto si è detto *supra* a proposito della pervasività del mezzo telematico nell'odierna esperienza dei diritti, non può aversi dubbio che l'accesso alla rete rappresenti oggi un'utilità fondamentale, la cui mancata o insufficiente disponibilità – che, come pure si è visto, per una parte non trascurabile della popolazione rappresenta uno scenario tutt'altro che meramente teorico – ostacola grandemente l'esercizio dei più vari diritti costituzionali. Pertanto, risponderebbe alla logica complessiva del sistema – che richiede di essere preservata proprio tenendo conto delle

29. C. cost., sent. n. 105/1972, punto 3 del Considerato in diritto. In senso analogo, in C. cost., sent. n. 225/1974, punto 5 del Considerato in diritto, si sostiene che «il diritto di “tutti” di manifestare liberamente il proprio pensiero con ogni mezzo di diffusione [...] non comprende anche quello di disporre di tutti i possibili mezzi».

30. Lo si osserva in COSTANZO 2012, p. 9.

31. Sul punto, anche con riferimento agli insegnamenti che devono trarsi dall'esperienza della crisi pandemica da Covid-19, D'IPPOLITO 2021, spec. p. 83, nonché LOTTA 2020, pp. 62-63.

32. In questo senso sembrano esprimersi DE MINICO 2011, spec. par. 1, e FROSINI 2011, p. 8. *Contra*, nel senso dell'inconfigurabilità, a Costituzione vigente, di un diritto sociale avente ad oggetto l'accesso alla rete, si veda CUOCOLO 2012, pp. 282-287, nonché BETZU 2012, pp. 6-8.

33. TANZARELLA 2021, p. 42.

trasformazioni della realtà sociale e dei meccanismi di distribuzione delle risorse che la caratterizzano – che detto accesso fosse reso oggetto di un espresso diritto costituzionale, formulato secondo il linguaggio e la sistematica dei diritti sociali³⁴.

Né può accettarsi l'obiezione secondo cui una simile revisione costituzionale, incidendo sulla Parte prima della Carta, aprirebbe la strada anche a future modifiche regressive dei diritti fondamentali³⁵. Ciò in primo luogo perché, ad oggi, modifiche di non secondario rilievo a disposizioni della Parte prima si sono già registrate, sicché la responsabilità di aver dato la stura ad eventuali ripensamenti in senso regressivo non potrebbe essere addossata all'intervento di revisione qui ipotizzato: si pensi – per limitarsi ad alcuni esempi – all'art. 51 Cost., integrato, ad opera della l. cost. n. 1/2003, con l'aggiunta di un secondo periodo che esprime il principio delle pari opportunità tra donne e uomini; oppure, più di recente, all'art. 41 Cost., cui la l. cost. n. 1/2022 ha aggiunto riferimenti alla «salute» e all'«ambiente» in funzione di limiti alla libertà di iniziativa economica privata, nonché ai «fini [...] ambientali» quale nuova categoria di scopi che la legge può imporre all'attività economica dei soggetti pubblici e privati³⁶. In secondo luogo, e soprattutto, perché quella qui sostenuta sarebbe – per così dire – una revisione costituzionale di tipo *conservativo*, volta a «rivitalizzare» il principio di eguaglianza sostanziale³⁷, nello specifico senso di

preservarne le valenze a fronte di un mutato scenario sociale, rendendone esplicita l'estensione all'accesso alla rete quale nuova utilità fondamentale emersa dal progresso tecnologico, e ciononostante disegualmente distribuita.

4. Il diritto (sociale) all'accesso alla rete: dall'art. 21-bis all'art. 34-bis Cost. (e ritorno)

Affermata così l'utilità della positivizzazione, in Costituzione, di una specifica situazione giuridica soggettiva, da configurare come diritto sociale all'accesso alle reti telematiche, il problema si sposta sulla formulazione delle relative disposizioni e sulla loro collocazione sistematica nel testo costituzionale. Sembra dunque utile dedicare le battute finali del presente contributo a qualche rapida riflessione sui diversi disegni di legge costituzionale, presentati nel corso di diverse legislature e sinora mai giunti ad approvazione definitiva, con i quali il decisore politico si è proposto di includere un simile diritto nel novero dei diritti fondamentali espressamente tutelati dalla Costituzione. Per la precisione, il riferimento è ai seguenti progetti di legge costituzionale:

- d.d.l. cost. A.S. n. 2485 (XVI legislatura);
- d.d.l. cost. A.S. n. 1317 (XVII legislatura);
- d.d.l. cost. A.S. n. 1561 (XVII legislatura);
- d.d.l. cost. A.C. n. 1136 (XVIII legislatura);
- d.d.l. cost. A.C. n. 327 (XIX legislatura)³⁸.

34. In tal senso MARSOCCI 2015, pp. 11-12. Ancorché formulate a sostegno di un intervento di revisione costituzionale volto non alla previsione di un diritto sociale a sé stante, bensì all'inserimento di riferimenti al cyberspazio negli artt. 2 e 3 Cost., nella stessa chiave risultano persuasive le considerazioni di ALLEGRI 2016, p. 24: secondo l'autrice, sebbene non possa ritenersi «del tutto scorretta la tesi per cui i principi già presenti in Costituzione – soprattutto gli artt. 2 e 3 Cost. – possano applicarsi senza difficoltà al cyberspazio», nondimeno «appare davvero singolare che una Costituzione non preveda norme specificamente riferite a questo nuovo ambiente così incredibilmente pervasivo e travolgente, in cui si svolge una amplissima parte (e forse presto anche la maggior parte?) della nostra vita esperienziale e relazionale».

35. DE MINICO 2011, cap. II, par. 1. Analogamente, una viva preoccupazione per uno scenario in cui «l'effettività dei principi costituzionali» sia posta «alla mercé del revisore costituzionale» è espressa – in aggiunta ad altre obiezioni, in estrema sintesi riconducibili all'esigenza di preservare il carattere «aperto» del testo costituzionale – da TANZARELLA 2021, p. 53.

36. Argomento, questo, che – con specifico riferimento all'esempio della modifica dell'art. 51 Cost. – si trova impiegato contro le tesi critiche da RODOTÀ 2012, p. 387.

37. Per questa formula MARSOCCI 2015, p. 12. Di «un classico intervento di «manutenzione» costituzionale» discorre invece AZZARITI 2011, par. 4.

38. Per una ricostruzione del dibattito su queste varie proposte si veda ALLEGRI 2016, p. 3 ss., nonché D'IPPOLITO 2021, p. 93 ss.

Vi è un primo dato che occorre sottolineare: di là dal dettaglio delle rispettive formulazioni, tutti i disegni di legge costituzionale citati, così come la già menzionata Dichiarazione dei diritti di Internet, parlano in qualche misura il linguaggio dei diritti sociali. Se il d.d.l. cost. A.S. n. 2485 (XVI legislatura) e il più recente d.d.l. cost. A.C. n. 327 (XIX legislatura) si limitano a richiamare la «rimozione degli ostacoli di ordine economico e sociale», gli altri testi sopra richiamati si lasciano apprezzare per il fatto di porre espressamente tale compito in capo ai pubblici poteri, mediante il chiaro riferimento alla Repubblica o – nel caso dell'art. 2, co. 5, della Dichiarazione – alle «Istituzioni pubbliche». Su questo fronte, le formulazioni più complete sembrano essere quella del d.d.l. cost. A.C. n. 1136 (XVIII legislatura) e quella dell'art. 2 della Dichiarazione, che chiariscono come la pretesa a prestazioni positive espressa dal diritto riguardi la connessione alla rete «con modalità tecnologicamente adeguate»; formula, questa, che sembra capace di adattarsi, in via di interpretazione evolutiva, ai futuri stadi del progresso tecnologico.

Se il richiamo al principio di eguaglianza sostanziale, quale fondamento assiologico della situazione giuridica di cui si prospetta la costituzionalizzazione, è chiaramente visibile in tutti i testi in parola, la principale divergenza attiene alla collocazione sistematica del nuovo diritto. Il d.d.l. cost. A.S. n. 2485 (XVI legislatura) e il d.d.l. cost. A.S. n. 1317 (XVII legislatura), infatti, inseriscono il diritto di accesso ad Internet rispettivamente in un nuovo art. 21-*bis* e nel co. 2 dell'art. 21 Cost. In tal modo, essi si mostrano tributari di

quell'impostazione originaria – cui si è fatto cenno *supra* (par. 3) – che concepiva il diritto di accesso alla rete come strettamente connesso alla libertà di manifestazione del pensiero, in quanto strumento dell'esercizio di quest'ultima³⁹. Diversamente, i successivi d.d.l. cost. A.S. n. 1561 (XVII legislatura) e d.d.l. cost. A.C. n. 1136 (XVIII legislatura) collocano il nuovo diritto in coda al Titolo II della Parte I della Costituzione, e pertanto nel bel mezzo della disciplina dei più tradizionali diritti sociali, in un nuovo art. 34-*bis*. Tale collocazione, unitamente alla qualificazione dell'«accesso alla rete Internet» come «luogo ove si svolge la personalità umana, si esercitano i diritti e si adempiono i doveri di solidarietà politica, economica e sociale», svincola il nuovo diritto dal tradizionale legame privilegiato con la libertà di manifestazione del pensiero, prendendo atto di come l'accesso rappresenti una risorsa necessaria per l'esercizio della generalità dei diritti previsti dalla Costituzione⁴⁰. Per le ragioni più volte illustrate in questo scritto, una simile concezione appare più condivisibile, e lo sarebbe a maggior ragione laddove l'evoluzione digitale del processo conducesse a qualificare l'accesso alle reti come utilità fondamentale *anche* per l'esercizio dei diritti di azione e di difesa.

In questa prospettiva, qualche critica può forse appuntarsi sul fatto che il d.d.l. cost. A.C. n. 327 (XIX legislatura), recuperando l'impostazione originaria, torni a concepire il diritto di accesso ad Internet quale strumento della sola libertà di manifestazione del pensiero, collocandolo in un nuovo ultimo comma dell'art. 21 Cost.

Riferimenti bibliografici

- M.R. ALLEGRI (2021), *Il diritto di accesso a Internet: profili costituzionali*, in “MediaLaws”, 2021, n. 1
- M.R. ALLEGRI (2016), *Riflessioni e ipotesi sulla costituzionalizzazione del diritto di accesso a Internet (o al ciber spazio?)*, in “Rivista AIC”, 2016, n. 1
- A. ANDREONI (2006), *Lavoro, diritti sociali e sviluppo economico. I percorsi costituzionali*, Giappichelli, 2006
- V. ATRIPALDI (1974), *Contributo alla definizione del concetto di partecipazione nell'art. 3 della Costituzione*, in Aa.Vv., “Strutture di potere, democrazia e partecipazione”, Editoriale Scientifica, 1974

39. Una lettura, questa, condivisa da AZZARITI 2011, par. 4.

40. In tal senso D'IPPOLITO 2021, pp. 97-102. Analogamente MARSOCCHI 2015, pp. 11-12.

- G. AZZARITI (2011), *Internet e Costituzione*, in “Costituzionalismo.it”, 2011, n. 2
- P. BARCELLONA (1994), *Diritti sociali e Corte costituzionale*, in “Rivista giuridica del lavoro e della previdenza sociale”, 1994, n. 2
- G. BELLAVISTA (1964), *Difesa giudiziaria penale*, in “Enciclopedia del diritto”, vol. XII, Giuffrè, 1964
- M. BETZU (2012), *Interpretazione e sovra-interpretazione dei diritti costituzionali nel cyberspazio*, in “Rivista AIC”, 2012, n. 4
- P. BIAVATI (2022), *La riforma del processo civile: motivazioni e limiti*, in “Rivista trimestrale di diritto e procedura civile”, 2022, n. 1
- P. BIAVATI (2021), *Processo civile e pandemia. Che cosa passa, che cosa rimane*, in “Rivista trimestrale di diritto e procedura civile”, 2021, n. 1
- G. BRONZINI (2021), *Il rito del lavoro del 1973 e le tentazioni cartolari e da remoto*, in “Rivista italiana di diritto del lavoro”, 2021, n. 1
- A. BUSACCA (2017), *“Diritto di accesso” alla rete Internet*, in “OIDU - Ordine Internazionale e Diritti Umani”, 2017, n. 3
- C. BUZZACCHI (2020), *La banda larga tra intervento pubblico e mercato*, in “Diritto Pubblico Europeo – Rassegna online”, 2020, n. 1
- Q. CAMERLENGO (2013), *Costituzione e promozione sociale*, il Mulino, 2013
- B. CARAVITA (1984), *Oltre l'eguaglianza formale. Un'analisi dell'art. 3 comma 2 della Costituzione*, Cedam, 1984
- M.A. CATTANEO (1999), *Uguaglianza*, in “Digesto delle discipline pubblicistiche”, Utet, 1999
- A. CERRI (1984), *Eguaglianza giuridica ed egualitarismo*, Japadre, 1984
- A. CLARONI (2021), *Mezzogiorno, banda larga e divario digitale. Profili normativi e questioni aperte*, in “Rivista giuridica del Mezzogiorno”, 2021, n. 1
- L.P. COMOGGIO (1981), *Art. 24, co. 1 e co. 2*, in G. Branca (a cura di), “Commentario della Costituzione”, Zanichelli, 1981
- P. COSTANZO (2012), *Miti e realtà dell'accesso ad internet (una prospettiva costituzionalistica)*, in “Consulta online”, 2012
- V. CRISAFULLI (1954), *Individuo e società nella Costituzione italiana*, in “Il diritto del lavoro”, 1954, n. 1
- L. CUOCOLO (2012), *La qualificazione giuridica dell'accesso a Internet, tra retoriche globali e dimensione sociale*, in “Politica del diritto”, 2012, n. 2-3
- A. D'ALOIA (2002), *Eguaglianza sostanziale e diritto diseguale. Contributo allo studio delle azioni positive nella prospettiva costituzionale*, Cedam, 2002
- G. D'IPPOLITO (2021), *Il diritto di accesso ad Internet in Italia: dal 21(-bis) al 34-bis*, in “MediaLaws”, 2021, n. 1
- G. DE MINICO (2016), *Net neutrality come diritto fondamentale di chi verrà*, in “Costituzionalismo.it”, 2016, n. 1
- G. DE MINICO (2011), *Diritti Regole Internet*, in “Costituzionalismo.it”, 2011, n. 2
- G. DE MINICO (2009), *Regulation, banda larga e servizio universale. Immobilismo o innovazione?*, in “Politica del diritto”, 2009, n. 4
- D. DE RADA (2023), *Il diritto all'accesso ad internet, tra valori costituzionali e difficoltà di esercizio* in “Giustiziavivile.com”, 2023, n. 5

- E.A.A. DEI-CAS (2023), *La partecipazione “parzialmente smaterializzata”: il grimaldello del consenso a favore dell’economia processuale*, in “La legislazione penale”, 2023, n. 2
- G. DI GASPARE (2008), *Il lavoro quale fondamento della Repubblica*, in “Diritto pubblico”, 2008, n. 3
- C. ESPOSITO (1954), *Eguaglianza e giustizia nell’art. 3 della Costituzione*, in Id., “La Costituzione italiana. Saggi”, Cedam, 1954
- G. FERRARA (1978), *Corte costituzionale e principio di eguaglianza*, in N. Occhiocupo (a cura di), “La Corte costituzionale tra norma giuridica e realtà sociale: bilancio di vent’anni di attività”, il Mulino, 1978
- P. FERRUA (1989), *Difesa (diritto di)*, in “Digesto”, Utet, 1989
- F. FICHERA (1974), *Spunti tematici intorno al nesso tra principi di eguaglianza e di partecipazione di cui all’art. 3, 2° comma, della Costituzione*, in Aa.Vv., “Strutture di potere, democrazia e partecipazione”, Editoriale Scientifica, 1974
- T.E. FROSINI (2011), *Il diritto costituzionale di accesso a Internet*, in “Rivista AIC”, 2011, n. 1
- B. GALGANI (2023), *Il processo penale telematico*, in “Diritto penale e processo”, 2023, n. 1
- M.S. GIANNINI (2016), *Lo Stato democratico-repubblicano, oggi*, in Id., “Per uno Stato democratico-repubblicano”, Edizioni di storia e letteratura, 2016
- M.S. GIANNINI (1979), *I pubblici poteri negli Stati pluriclasse*, in “Rivista trimestrale di diritto pubblico”, 1979, n. 2-3
- A. GIORGIS (1999), *La costituzionalizzazione dei diritti all’uguaglianza sostanziale*, Jovene, 1999
- U. GOLDONI, R. REALI (1988), *Difesa e autodifesa*, in “Enciclopedia giuridica”, Istituto dell’Enciclopedia italiana, 1988
- C. LAVAGNA (1977), *Costituzione e socialismo*, il Mulino, 1977
- C. LOTTA (2020), *Un nuovo diritto al tempo del Covid-19? Accesso a Internet e digital divide*, in “Rivista del Gruppo di Pisa”, 2020, n. 2
- M. LUCIANI (1995), *Titolo III – Rapporti economici*, in G. Neppi Modona (a cura di), “Stato della Costituzione. Principi, regole, equilibri. Le ragioni della storia, i compiti dell’oggi”, Il Saggiatore, 1995
- P. MARSOCCI (2015), *Cittadinanza digitale e potenziamento della partecipazione politica attraverso il web: un mito così recente già da sfatare?*, in “Rivista AIC”, 2015, n. 1
- E. MONTAGNANI (2022), *Le pubbliche amministrazioni nell’era delle tecnologie cloud ed edge computing tra opportunità e rischi: il Piano Nazionale di Ripresa e Resilienza e le comunità digitali*, in “Rivista italiana di informatica e diritto”, 2022, n. 1
- C. MORTATI (1975), *Art. 1*, in G. Branca (a cura di), “Commentario della Costituzione”, Zanichelli, 1975
- L. NANNIPIERI (2013), *Costituzione e nuove tecnologie: profili costituzionali dell’accesso ad Internet*, in “Rivista del Gruppo di Pisa”, 2013, n. 3
- V. NARDO (2023), *La progressiva digitalizzazione del processo*, in “Processo penale e giustizia”, 2023, n. 1x
- C. PANSINI (2019), *Diritto di difesa e struttura del processo*, in “Processo penale e giustizia”, 2019, n. 2
- B. PEZZINI (2001), *La decisione sui diritti sociali. Indagine sulla struttura costituzionale dei diritti sociali*, Giuffrè, 2001
- L. PICCININNI (2023), *Le nuove norme in tema di giustizia digitale*, in “Rivista di diritto processuale”, 2023, n. 3
- A. PIZZORUSSO (1993), *Eguaglianza (diritto)*, in “Enciclopedia delle scienze sociali”, vol. II, Treccani, 1993

- A. PIZZORUSSO (1987), *Eguaglianza e libertà nella politica del diritto*, in “Studi in onore di P. Biscaretti di Ruffia”, vol. II, Giuffrè, 1987
- A. PIZZORUSSO (1983), *Che cos'è l'eguaglianza. Il principio etico e la norma giuridica nella vita reale*, Editori Riuniti, 1983
- A. POGGI (2020), *Diritto a internet o diritto alla libertà di manifestazione del pensiero?*, Aa.Vv., “Liber amicorum per Pasquale Costanzo - Diritto costituzionale in trasformazione”, I, Costituzionalismo, Reti e Intelligenza artificiale, in “Consulta OnLine”, 2020
- G.G. POLI (2023), *Il processo senza voce: considerazioni a margine della trattazione cartolare delle udienze civili (I)*, in “Il giusto processo civile”, 2023, n. 3
- A. POLICE (2008), *Art. 24*, in R. Bifulco, A. Celotto e M. Olivetti (a cura di), “Commentario alla Costituzione”, Utet, 2008
- G.U. RESCIGNO (1999), *Il principio di eguaglianza nella Costituzione italiana*, in Associazione Italiana dei Costituzionalisti, “Annuario 1998 – Principio di eguaglianza e principio di legalità nella pluralità degli ordinamenti giuridici. Atti del XIII Convegno Annuale”, Cedam, 1999
- R. RIZZUTO (2022), *L'efficienza costituzionalmente orientata e la digital transformation della giustizia penale*, in “Processo penale e giustizia”, 2022, n. 3
- S. RODOTÀ (2014), *Recensione a Giovanna De Minico, “Internet. Regola e anarchia”*, in “Diritto pubblico”, 2014, n. 1
- S. RODOTÀ (2012), *Il diritto di avere diritti*, Laterza, 2012
- U. ROMAGNOLI (1975), *Art. 3, co. 2*, in G. Branca (a cura di), “Commentario della Costituzione”, Zanichelli, 1975
- C. ROSSANO (2006), *Eguaglianza*, in S. Cassese (a cura di), “Dizionario di diritto pubblico”, vol. III, Giuffrè, 2006
- C. ROSSANO (2005), *Profili dell'eguaglianza sostanziale nella Costituzione italiana e nell'ordinamento comunitario*, in “Studi in onore di G. Ferrara”, vol. III, Giappichelli, 2005
- A. ROSSETTI (2011), *È necessario il diritto all'accesso alla rete?*, in M. Pietrangelo (a cura di), “Il diritto di accesso ad Internet”, Edizioni scientifiche italiane, 2011
- S. SATTA (1959), *Azione (dir. pos.)*, in “Enciclopedia del diritto”, vol. IV, Giuffrè, 1959
- M. SCAPARONE (1981), *Art. 24, co. 2 – Il diritto di difesa nel processo penale*, in G. Branca (a cura di), “Commentario della Costituzione”, Zanichelli, 1981
- F. SORRENTINO (2011), *Eguaglianza. Lezioni*, Giappichelli, 2011
- P. TANZARELLA (2021), *L'accesso a Internet è fondamentale, ma è davvero un diritto (fondamentale)?*, in “MediaLaws”, 2021, n. 1
- P. TANZARELLA (2013), *Accesso a Internet: verso un nuovo diritto sociale?*, in E. Cavasino, G. Scala, G. Verde (a cura di), “I diritti sociali dal riconoscimento alla garanzia. Il ruolo della giurisprudenza. Atti del Convegno di Trapani”, Editoriale Scientifica, 2013
- P. TONINI (2022), *Le nuove tecnologie e la riforma Cartabia*, in “Diritto penale e processo”, 2022, n. 3
- G.P. VOENA (1988), *Difesa penale*, in “Enciclopedia giuridica”, Istituto dell'Enciclopedia italiana, 1988
- P. ZUDDAS (2020), *Covid-19 e digital divide: tecnologie digitali e diritti sociali alla prova dell'emergenza sanitaria*, in “Osservatorio costituzionale”, 2020, n. 3

Sezione monografica

Minori e Internet

a cura di

Carlo Colapietro e Antonio Iannuzzi



CARLO COLAPIETRO – ANTONIO IANNUZZI

I diritti dei minori nella società digitale tra profili di responsabilità ed esigenze di protezione

La pervasività del digitale nel contesto sociale chiama i giuristi, e non soltanto essi, ad una riflessione sulle modalità di tutela di diritti dei minori online. Essi, infatti, risultano esposti in modo particolare, in quanto considerati soggetti vulnerabili, ai cosiddetti “pericoli” della Rete e perciò occorre esaminare con attenzione e approccio metodologico rigoroso quelle che possono considerarsi le principali implicazioni giuridiche, etiche e sociali che derivano dalla presenza nell’ambiente digitale dei minorenni. Tra questi, senza dubbio, la tutela della riservatezza dei minori, la verifica della loro età nella fase di accesso e di utilizzo di applicativi online, la responsabilità diretta dei genitori o di chi funge da tutore dei minorenni nonché, da ultimo, lo sfruttamento economico e commerciale dei cosiddetti “baby influencer”. Al centro della riflessione, connotata per la sua multidisciplinarietà, resta l’importanza di approdare ad una regolamentazione che sappia valorizzare tanto l’importanza degli strumenti educativi quanto il bilanciamento dei diritti e delle libertà in gioco, a partire dalla libertà di espressione, dalla tutela della riservatezza e dalla libertà di iniziativa economica privata sulla quale si basa lo sviluppo tecnologico.

Diritti dei minori – Società digitale – Protezione dei dati – Verifica dell’età – Responsabilità genitoriale

Sharenting and children's data protection: legal aspects of an interdisciplinary phenomenon

The pervasiveness of digital technology in the social context calls on legal experts – and not only them – to reflect on how to protect children’s rights online. Minors are particularly exposed, as they are considered vulnerable individuals, to online risks. Therefore, it is essential to carefully and methodically examine the primary legal, ethical, and social implications arising from the presence of minors in the digital environment. These include the protection of minors’ privacy, age verification during access to and use of online applications, the direct responsibility of parents or guardians, and, at last, the economic and commercial exploitation of so-called “baby influencers.” At the heart of this multidisciplinary reflection lies the importance of achieving a regulatory framework that enhances the value of educational tools while balancing the rights and freedoms at stake, including freedom of expression, the protection of privacy, and the freedom of private economic initiative underpinning technological development.

Children’s rights – Digital society – Data protection – Age verification – Parental responsibility

Gli Autori sono professori ordinari di Istituzioni di diritto pubblico presso l’Università degli Studi Roma Tre

Il presente contributo introduttivo è frutto della riflessione comune e della collaborazione dei due Autori, curatori della sezione monografica; tuttavia, il paragrafo 1 è stato scritto da Antonio Iannuzzi e il paragrafo 2 da Carlo Colapietro

Questo contributo fa parte della sezione monografica *Minori e Internet* a cura di Carlo Colapietro e Antonio Iannuzzi

1. Anche gli osservatori più distratti si sono ormai accorti che la dimensione digitale sta avvolgendo l'esperienza umana, modificando o ampliando la sede di manifestazione dei diritti costituzionali. Lo ha affermato chiaramente la Corte costituzionale a proposito dell'interpretazione attuale del diritto di corrispondenza: «La garanzia [costituzionale, ndr] si estende (...) ad ogni strumento che l'evoluzione tecnologica mette a disposizione a fini comunicativi, compresi quelli elettronici e informatici, ignoti al momento del varo della Carta costituzionale». In proposito, ha aggiunto ancor più chiaramente che «la nozione di “corrispondenza” – utilizzata anche nell'art. 68, terzo comma, Cost. senza ulteriore specificazione – appare, tuttavia, sufficientemente ampia da ricomprendere le forme di scambio di pensiero a distanza (...) costituenti altrettante “versioni contemporanee” della corrispondenza epistolare e telegrafica. Sostenere il contrario, in un momento storico nel quale la corrispondenza cartacea, trasmessa tramite il servizio postale e telegrafico, è ormai relegata, nel complesso, a un ruolo di secondo piano, significherebbe d'altronde deprimere radicalmente la valenza della prerogativa parlamentare in questione»¹. In altre parole, cambia il luogo in cui si esercita il diritto, ma non muta né l'essenza del diritto in questione né la garanzia costituzionale apprestata².

Tale posizione, di portata senz'altro generale, si estende alla realtà che coinvolge i soggetti minori d'età, i quali – in quanto “nativi” digitali – sono costantemente immersi in una dimensione cibernetica totalizzante e capace di permeare (e persino invadere) ogni aspetto della loro vita, a partire dalle formazioni sociali ove essi formano la propria personalità in modo prevalente: la scuola e la famiglia.

La tutela nei confronti dei diritti dei minori in Rete, in quanto soggetti deboli o vulnerabili, deve essere speciale e rafforzata³.

A partire da questo assunto, che funge da presupposto di tutte le argomentazioni giuridiche accolte in questa sezione monografica, occorre concentrarsi sul punto di caduta del massiccio coinvolgimento dei minori nello spazio virtuale, rappresentato dalla presenza di importanti e delicate implicazioni giuridiche e sociali che richiedendo un ripensamento, a livello strutturale, dei sistemi di tutela dei diritti dei minori online, cui deve necessariamente affiancarsi una precipua regolamentazione basata su una lettura costituzionalmente orientata dei diritti e delle libertà che si incrociano nel fenomeno sociale dello sviluppo umano e tecnologico.

L'ambiente digitale, infatti, senza dubbio offre ai più giovani (ma non soltanto, lo si è detto) opportunità di apprendimento, e di diffusione delle conoscenze acquisite, potenzialmente sconfinata, ma è proprio tale ampiezza a determinare una serie di rischi specifici che coinvolgono i soggetti minori più vulnerabili, i quali, pienamente immersi nel loro percorso di formazione, spesso e volentieri non risultano ancora dotati di strumenti sufficienti a consentirgli di distinguere le fonti di informazione, di testare e vagliare la veridicità e affidabilità di quanto acquisito e immesso dalla Rete e in Rete nonché di comprendere appieno il grado valoriale di condotte e comportamenti che facilmente si apprestano ad emulare (una dinamica, questa, sulla quale d'altronde si fonda il meccanismo di conoscenza proprio di tutti gli esseri umani).

Da questo punto di vista, non soltanto si pone un immediato problema circa la “qualità” dei

1. Corte cost., sent. n. 170/2023.

2. Per un approfondimento di questa posizione teorica con evidenti ricadute pratiche in termini di tutela dei diritti fondamentali si rinvia a IANNUZZI-LAVIOLA 2023, n. 1, p. 9 ss.

3. Sul punto si v. almeno OROFINO-PIZZETTI 2018.

contenuti che circolano attraverso Internet, che comporta un immediato e correlato rischio di esporre il minore a contenuti dannosi o inadeguati per la propria età, ma anche un profilo – assai rilevante – che riguarda l’acquisizione di dati e informazioni direttamente o indirettamente riconducibili al minore. Difatti, oggi è evidente la facilità con la quale i dati personali facenti capo ai minori possano essere acquisiti, processati e impiegati per alimentare i processi di machine learning con finalità di profilazione di natura predittiva o prescrittiva, esponendo concretamente i minori a fenomeni di sfruttamento commerciale o, peggio ancora, di cyberbullismo.

Alcuni fenomeni emergenti, inoltre, rappresentano una manifestazione tangibile delle implicazioni economiche e sociali dell’utilizzo della Rete da parte dei minori. Il caso lampante è quello dei cosiddetti “baby influencer”, spesso al centro di strategie di marketing digitale fondate sullo sfruttamento della loro immagine e dei loro dati, sollevando problemi molto delicati al confine tra l’etica e il diritto.

In questo contesto, pertanto, il bilanciamento dei diritti del minore è elemento cruciale: la riservatezza del minore e il diritto alla sua protezione debbono essere garantiti e assicurati in modo pieno, senza che siano compromesse le esigenze di sviluppo del mercato digitale. Quest’ultimo non a caso dovrebbe contraddistinguersi per la sua sicurezza, la sua affidabilità, la sua sostenibilità e, da ultimo, per la sua accessibilità condizionata al rispetto dell’età laddove siano coinvolti i minorenni e siano in gioco contenuti sensibili e a loro inadatti.

Ecco, quindi, che un aspetto centrale e particolarmente delicato è rappresentato dall’esigenza di predisporre sistemi efficaci di *age verification*, ossia strumenti volti ad assicurare che l’età dichiarata dall’utilizzatore del servizio possa essere verificata inequivocabilmente e ciò proprio al fine di proteggere i minori dall’accesso a contenuti non adeguati.

Sotto il profilo normativo, l’articolo 8 del Regolamento UE 679/2016 (rubricato “Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell’informazione”) pone le basi per l’accesso dei minori ai servizi di quella che è definita la «società dell’informazione», ma la previsione del secondo paragrafo secondo la quale «Il titolare del trattamento si adopera in ogni modo

ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili» non è affatto di facile attuazione e, meno che meno, di facile verificabilità. La legislazione nazionale, emblematicamente sfociata nel più recente decreto-legge “Caivano” (15 settembre 2023, n. 123), ha sì introdotto obblighi specifici per i gestori delle piattaforme digitali, ma il quadro normativo risulta complessivamente ancora frammentario, con implicazioni tecniche e giuridiche che restano tutte da esplorare, il che trova una sua evidenza nelle copiose decisioni delle autorità indipendenti che hanno a più riprese sanzionato i prestatori di servizi cui accedono anche (e talvolta soprattutto) i minorenni, incapaci di assicurare che la verifica dell’età sia svolta in modo effettivo e non soltanto formale.

A fronte di un’accelerazione tecnologica senza precedenti, tuttavia, la risposta normativa non può essere l’unica, ma occorre mettere in atto una serie di azioni coordinate fondate su una vera e propria educazione digitale e al digitale, seguendo un approccio che massimizzi le opportunità e, al contempo, riduca al minimo i rischi.

2. Venendo al merito del contenuto di questa sezione monografica, esso aspira ad essere un contributo al dibattito che origina dalla totale immersione dei minorenni nel contesto digitale e si basa su un approccio multidisciplinare volto ad affrontare le principali questioni problematiche connesse alla protezione dei minori nell’ambiente digitale.

Il saggio di Simonetta Trozzi (*La tutela dei minori nel prisma della protezione dei dati personali. I sistemi di verifica dell’età tra personalismo ed esigenze di bilanciamento fra diritti*), che apre la sezione, analizza il rapporto che intercorre tra i diversi sistemi di *age verification* e la disciplina generale della protezione dei dati personali, con particolare riguardo alle norme contenute nel GDPR 679/2016. Al centro, l’autrice pone la necessità di un intervento normativo armonizzato che riesca a garantire un’efficace tutela dei minori nello spazio digitale dedicando ampio spazio ai principi di proporzionalità e all’esigenza di limitazione della finalità del trattamento dei dati, sulla base di un delicato bilanciamento tra protezione e circolazione dei dati che dovrebbe costituire il cuore della regolamentazione.

Segue un contributo di Francesca Ricciulli (*L'identità e l'identificazione digitale del minore tra normativa nazionale e internazionale e i provvedimenti delle autorità competenti*), la quale esamina, invece, i futuri scenari normativi e applicativi derivanti dall'adozione di strumenti di *age assurance*, prendendo le mosse dal recente schema di Regolamento elaborato dall'AGCOM in attuazione del già menzionato decreto-legge "Caivano". L'autrice, in particolare, approfondisce le intersezioni tra le disposizioni normative nazionali in materia di protezione dei diritti dei minori online e il Regolamento europeo "eIDAS 2", con un focus sui rischi e le opportunità legati all'introduzione di un'identità digitale sicura e interoperabile a tutela dei minori.

Il contributo di Giovanni Barozzi Reggiani (*Protezione dei minori dai contenuti nocivi circolanti sulle Video Sharing Platforms: un'ipotesi di (ir)ragionevolezza legislativa?*) si concentra, per parte sua, sulle cosiddette *video sharing platforms* (VSP), offrendo un'analisi che pone al centro il bilanciamento tra la protezione dei minori in Rete da contenuti inappropriati e la protezione di diritti costituzionalmente rilevanti come la libertà di manifestazione del pensiero e la libertà di iniziativa economica. Lo studio dell'autore si estende, infine, alle competenze attribuite all'AGCOM dal Testo Unico dei servizi media audiovisivi, proponendo una riflessione critica sulla razionalità delle misure adottate e sulla necessità di un approccio regolatorio fondato su evidenze di natura scientifica.

Proseguendo, Dorinda Caccioppo (*Sharenting e tutela dei dati personali del minore: profili giuridici di un fenomeno interdisciplinare*) affronta la questione del cosiddetto *sharenting*, vale a dire la pratica, messa in atto dai genitori o da coloro che detengono la responsabilità del minore, di condividere informazioni sui propri figli (o sui minori loro affidati) online. Il caso emblematico è quello della condivisione sui social network di immagini che ritraggono i soggetti minori. L'autrice del saggio esplora le implicazioni giuridiche di tale fenomeno, ponendo a confronto la normativa italiana e quella francese, richiamando, in conclusione, l'esigenza di un delicato equilibrio tra la libertà di espressione dei genitori e la tutela dei minori a partire dalla specifica tutela dei dati personali dei minorenni.

Il contributo di Domiziano Pierantoni (*Minori su Internet: profili di responsabilità*) si focalizza, invece, su tutti quei profili di responsabilità che

derivano dall'utilizzo della Rete da parte dei minori, evidenziando l'importanza di svolgere adeguate e precise azioni di natura preventiva che costituiscano un'educazione civica al digitale. Al centro della propria analisi, l'autore pone il principio del *best interest of the child*, mettendo in luce l'esigenza di una collaborazione sinergica e attiva tra genitori, enti, istituzioni e prestatori di servizi digitali, i quali, tutti insieme, si impegnino a garantire un'esperienza online sicura e consapevole per i minori.

Benedetta Agostinelli (*Autonomia e controllo dei minori on line. I nuovi confini della responsabilità genitoriale*), dal canto suo, svolge un approfondimento ulteriore del tema della responsabilità genitoriale, analizzata sotto il profilo giusprivatistico, affermando come, da un lato, l'evoluzione delle tecnologie e, dall'altro, la stratificazione delle disposizioni normative sul trattamento dei dati personali riescano ad incidere sulla capacità di controllo dei genitori. L'autrice, non a caso, analizza le implicazioni di questa nuova realtà digitale, concludendo sull'importanza di strumenti educativi e normativi che rafforzino il ruolo genitoriale senza compromettere i diritti fondamentali dei minori.

Infine, il contributo di Lorenzo Maria Lucarelli Tonini (*Strumenti di age verification alla luce del contributo del Garante privacy e dell'AGCOM: il rischio di obsolescenza tecnologica e conoscitiva*) offre una panoramica delle problematiche connesse alla verifica dell'età dei minori, esaminando le disposizioni normative e i provvedimenti emanati dalle autorità competenti, con particolare attenzione agli strumenti di *age verification* e ai requisiti richiesti per garantire un'efficace tutela rafforzata nel contesto digitale.

Questa sezione monografica, in conclusione, vorrebbe collocarsi al confine tra la riflessione giuridica teorica e l'effettività che contraddistingue la predisposizione di strumenti concreti che tutelino i minorenni nello spazio digitale, ponendo, si spera, qualche punto fermo nella riflessione, che possa aiutare ad affrontare le sfide emergenti e sempre più ingombranti poste dall'incessante trasformazione tecnologica, con l'obiettivo di tutelare i diritti dei minori e promuovere un uso responsabile e consapevole della Rete.

Riferimenti bibliografici

- A. IANNUZZI, F. LAVIOLA (2023), *I diritti fondamentali nella transizione digitale fra libertà e uguaglianza*, in “Diritto costituzionale”, 2023, n. 1
- M. OROFINO, F. PIZZETTI (a cura di) (2018), *Privacy, minori e cyberbullismo*, Giappichelli, 2018



SIMONETTA TROZZI

La tutela dei minori nel prisma della protezione dei dati personali. I sistemi di verifica dell'età tra personalismo ed esigenze di bilanciamento fra diritti

Il saggio analizza il rapporto tra i sistemi di controllo dell'età degli utenti dei servizi online e la disciplina della protezione dei dati personali. Il Regolamento (UE) 2016/679 costituisce al tempo stesso il fondamento della tutela del minore nella società digitale, con riguardo all'accesso ai servizi della società dell'informazione, nonché misura della legittimazione del trattamento dei propri dati personali per scopi di verifica dell'età. A tal fine l'analisi trae spunto dai requisiti, quali l'implicito canone di proporzionalità sotteso alla verifica dell'età, che emergono dall'applicazione del principio di limitazione della finalità del trattamento. Solamente un intervento di armonizzazione normativa che renda obbligatoria la verifica dell'età per tutti i servizi della società dell'informazione potrà restituire pienezza al carattere relazionale che connota la tutela del minore, anche nella società digitale. L'attendibilità e il rischio associati al meccanismo di verifica dell'età così individuato dipenderanno, dunque, nel sistema multilivello di tutela dei diritti, dal bilanciamento tra le esigenze della circolazione e della protezione dei dati personali, che fondano lo statuto della protezione della persona nella dimensione digitale.

*Tutela dei dati personali – Sistemi per la verifica dell'età dell'utente – Limitazione della finalità del trattamento
Diritti dei minori – Costituzionalismo digitale*

The protection of minors within the framework of personal data protection. Age verification systems between personalism and balancing of rights

The essay analyzes the relationship between age verification systems and the framework of personal data protection. Regulation (EU) 2016/679 serves as both the foundation for the protection of minors in digital society and the legitimacy principle governing the use of their personal data for age verification purposes. To this end, the analysis will draw on issues arising from the application of the purpose limitation principle, such as the implicit standard of proportionality underlying age verification, and related challenges. Only a regulatory harmonization effort to mandate the age verification for all information society services could restore the relational nature that characterizes the protection of minors in the digital society. The reliability as much as the risks of the mechanism will thus depend upon the balancing of data circulation and personal data protection within the multilevel system of fundamental right protection. These two pillars constitute the core normative framework protecting the individual in digital societies.

Personal data protection – Age verification – Purpose limitation – Children's rights – Digital constitutionalism

L'Autrice è dottoranda di ricerca in Legalità, culture politiche e democrazia presso l'Università degli Studi di Perugia
Questo contributo fa parte della sezione monografica *Minori e Internet* a cura di Carlo Colapietro e Antonio Iannuzzi

SOMMARIO: 1. Premessa. L'accesso dei minori ai contenuti e ai servizi online: frammentarietà e mutamento dello scenario tecnologico e giuridico. Il GDPR quale *fulcro* della regolazione europea della società digitale. – 2. Alcuni chiarimenti definitivi: *l'age gate* e *l'age appropriate design*. La dimensione relazionale della tutela dei diritti del minore nella dimensione offline e in quella online. – 3. I sistemi di assicurazione dell'età alla luce della finalità del trattamento. Il canone della proporzionalità sotteso alla verifica del c.d. consenso digitale. – 3.1. *Il bilanciamento tra diritti e il criterio di ragionevolezza: i cardini della disciplina delle nuove tecnologie. La sentenza della Corte costituzionale n. 69 del 2024.* – 4. Conclusioni. La sfida complessa di un'armonizzazione necessaria a livello europeo (GDPR, DSA) e nazionale.

1. Premessa. L'accesso dei minori ai contenuti e ai servizi online: frammentarietà e mutamento dello scenario tecnologico e giuridico. Il GDPR quale *fulcro* della regolazione europea della società digitale

Nel gennaio 2024 è stata istituita, da parte della Commissione europea, una *task force* sulla verifica

dell'età per dare attuazione al Regolamento (UE) 2022/2065 (Regolamento sui servizi digitali o DSA)¹, con lo scopo precipuo di individuare un approccio comune Ue sui sistemi di verifica dell'età degli utenti dei servizi digitali, ossia dei servizi della società dell'informazione², noti come sistemi di *age verification* (verifica dell'età), talvolta indicati – come si vedrà – anche tramite la locuzione

1. Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) adottato per salvaguardare il mercato europeo dei servizi di intermediazione digitale, garantire anche online il godimento dei diritti fondamentali sanciti nella Carta dei diritti fondamentali dell'Unione, proteggere i diritti dei consumatori in rapporto alla fruizione dei servizi della società dell'informazione e contrastare la diffusione di contenuti illegali. A tal fine sono stabiliti obblighi fondamentali applicabili a tutti i prestatori di servizi intermediari online, ossia i fornitori di piattaforme online, nonché obblighi supplementari sia per per i prestatori di piattaforme online «di dimensioni molto grandi» e di motori di ricerca online «di dimensioni molto grandi», nonché per tutti quelli che non sono microimprese o piccole imprese. L'obiettivo di ridurre la distanza tra la tutela del minore nell'ambiente offline e la sicurezza del medesimo nell'ambiente online (Considerando 12 e 40), con specifico riguardo alla verifica dell'età dell'utente, è considerata all'art. 28 – tra le disposizioni applicabili a tutti i fornitori di piattaforme online – e all'art. 35, paragrafo 1, lettera j) DSA – tra gli obblighi supplementari. Ai sensi dell'articolo 35, paragrafo 1, lettera j) del DSA, i fornitori di piattaforme online «di dimensioni molto grandi» (*Very Large Online Platforms* o *VLOPs*) e di motori di ricerca online «di dimensioni molto grandi» (*Very Large Online Search Engines* o *VLOSEs*), come designate con decisione della Commissione europea, devono adottare misure di attenuazione dei rischi sistemici, tra cui «misure mirate per tutelare i diritti dei minori, compresi strumenti di verifica dell'età e di controllo parentale, o strumenti volti ad aiutare i minori a segnalare abusi o ottenere sostegno, a seconda dei casi».
2. L'art. 4, par. 25 del Regolamento (UE) 2016/679 (GDPR) rinvia all'art. 1, par. 1 lett. b) della direttiva 2015/1535 che descrive il servizio della società dell'informazione come qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi.

age assurance (assicurazione dell'età). Tali sistemi consistono in metodi di controllo dell'età, improntati al principio di indipendenza e neutralità³, che nella pratica, generalmente, funzionano sulla base della richiesta all'utente dei servizi online di fornire un'attestazione d'identità ufficiale dalla quale vengono estratte le informazioni legate all'età, avvalendosi anche di processi di identificazione digitale quali l'identità digitale. Tra questi vi è l'identità digitale europea di cui al Regolamento (UE) 2014/910 oggetto di una recente innovazione dovuta all'entrata in vigore del Regolamento (UE) 2024/1183 meglio noto come Regolamento sulla creazione di un portafoglio europeo di identità digitale o EUID (*Electronic Identification*) o Regolamento sull'*e-ID*⁴.

L'obiettivo che si affida al presente saggio è quello di fare luce sulle istanze di tutela dei diritti del minore sottese al concreto operare dei meccanismi di verifica dell'età alla luce della disciplina della protezione dei dati personali. Dopo aver ricostruito il quadro normativo del Regolamento (UE) 2016/679 (d'ora in avanti, GDPR⁵) concernente l'accesso ai servizi della società dell'informazione (art. 8 GDPR), si farà ricorso al principio della finalità del trattamento (art. 5, par. 1, lett. b) GDPR). Tale principio trova fondamento nell'art. 8 par. 2 della Carta di Nizza, nucleo della tutela del diritto alla protezione dei dati di carattere personale⁶, che annovera lo stesso tra i diritti fondamentali e sancisce che affinché il trattamento sia legittimo esso debba avvenire *per finalità determinate, secondo il principio di lealtà oltre che in base al consenso*

3. Ossia processi che si basano sull'intervento di un intermediario indipendente nonché scelto dal fornitore del servizio online sul quale ricade l'obbligo della verifica. Si tratta di un'opzione considerata da molte piattaforme ma anche dalla maggior parte dei Paesi dove sono state prese iniziative il cui meccanismo adottato o di prossima adozione è quello previsto dalla legge. Tra questi vi è la Spagna dove l'Agencia Española de Protección de Datos (AEPD) ha sviluppato un Decalogo di principi relativo ai requisiti dei sistemi di verifica dell'età a seguito di una consultazione pubblica avviata nel contesto della legge spagnola 13/2022 del 7 luglio sulla comunicazione audiovisiva (Ley General de Comunicación Audiovisual). Si v. inoltre lo studio UNITED NATIONS SAFE ONLINE 2024.
4. Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio dell'11 aprile 2024 che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale. La novella è volta alla creazione di uno strumento europeo di identità digitale armonizzato esteso al settore privato e basato sullo strumento del portafoglio europeo di identità digitale (*EUDI wallet*). Nell'ambito dei processi di identificazione digitale, invero, non mancano altresì interventi degli attori privati, come rilevato nel provvedimento di avvertimento dell'Autorità garante per la protezione dei dati personali (provvedimento del 21 marzo 2024, doc-web n. 9998877) relativo al protocollo *Worldcoin*, associato a una rete finanziaria basata su una criptovaluta, ideato con l'obiettivo di creare un'identità digitale a livello globale (*World ID*) bastato un sistema di identificazione digitale che si avvale della scansione biometrica dell'iride. Riflette sulla locuzione «poteri privati» e indaga le ragioni per le quali «i processi di digitalizzazione, con particolare riferimento sia alla preliminare capacità di raccogliere e concentrare i dati, sia allo sviluppo dei sistemi idonei *per mettere a frutto i patrimoni informativi* così costituiti, si siano finora dispiegati nell'ambito del settore privato, che è in effetti il protagonista della rivoluzione digitale». PONTI 2023-B, p. 599. V. anche CARLONI 2015 e FALCONE 2023.
5. Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).
6. Il fondamento della tutela del diritto alla protezione dei dati personali si riviene nell'art. 8 della Carta dei diritti fondamentali dell'UE (Carta di Nizza) nonché nell'art. 16 del Trattato sul funzionamento dell'Unione europea. In entrambe, ai rispettivi par. 1, si riscontra l'enunciato per cui «[o]gni persona ha diritto alla protezione dei dati di carattere personale che la riguardano». La tutela della riservatezza e del trattamento dei dati personali inizia ad affermarsi in Europa attraverso la lettura dell'art. 8 Convenzione europea dei diritti dell'uomo ad opera dei giudici di Strasburgo nonostante detta disposizione non abbia un contenuto specificatamente dedicato ai menzionati aspetti ma alla vita privata e familiare.

della persona interessata o a un altro fondamento legittimo previsto dalla legge.

La prospettiva è quella di saggiare parallelamente quale bilanciamento tra le due esigenze, della circolazione e della protezione dei dati personali, è sotteso alla creazione e al funzionamento di tali sistemi, interrogandosi sui margini di compatibilità degli stessi con la tutela dei diritti dell'interessato prevista dal GDPR.

Come è noto, le esigenze della circolazione dei dati non sono estranee al GDPR, sebbene nell'applicazione successiva alla sua adozione le ragioni della *data protection* abbiano prevalso. Come si vedrà, dunque, in rapporto a tale specifico aspetto, il Regolamento offre un nucleo di tutela per i diritti del minore online che necessita di una integrazione ulteriore, nel solco di quella già prevista nel DSA⁷. Ciò a fronte anche della recente attuazione dei regolamenti adottati nell'ambito della *Strategia europea per i dati* della Commissione europea⁸, il cui scopo è agevolare ed incentivare il flusso della condivisione dei dati nei casi in cui ciò possa avvenire nella cornice di legittimità delle norme poste a presidio della protezione dei dati personali.

Non esiste, ad oggi, una locuzione né tantomeno una definizione comunemente adottata a livello europeo che valga a identificare un sistema di assicurazione dell'età. Con riguardo all'obbligo del prestatore del servizio, nonché titolare del trattamento, di accertare che il consenso sia prestato o

autorizzato dal titolare della responsabilità genitoriale, il GDPR statuisce che quest'ultimo deve adoperarsi «in ogni modo ragionevole» e «in considerazione delle tecnologie disponibili» (art. 8, par. 2 GDPR).

La rassegna delle plurime soluzioni tecniche volte a verificare l'età presenti sul mercato non solo mette in luce l'asincronia della regolazione in materia rispetto alle tecnologie disponibili ma anche la mancanza di una scelta condivisa che possa anche terminologicamente uniformare gli strumenti di attuazione degli obblighi di verifica dell'età che discendono dai plurimi atti di regolazione europea⁹. Tra questi, oltre ai richiamati DSA e GDPR, la Direttiva (UE) 2010/13 nota come Direttiva europea sui servizi media audiovisivi (da ora, AVMSD)¹⁰. Tali atti impongono *de iure condito* e *de iure condendo* agli Stati membri l'adozione e l'attuazione di tali misure di tutela del minore online, che avverranno in base al margine di manovra ad essi riservato.

Il quadro normativo è venuto peraltro ad arricchirsi dopo la pubblicazione del Regolamento (UE) 2024/1689, noto come AI Act. Ciò in rapporto alla possibilità di impiegare sistemi algoritmici di intelligenza artificiale anche coniugati al trattamento di dati biometrici¹¹.

Inoltre, con riguardo alle risultanze della *task force* della Commissione europea richiamata, è recente la scelta di favorire precipuamente processi

7. Il regolamento è stato adottato in combinazione con il Regolamento (UE) 2022/1925 sui mercati digitali (*Digital Markets Act*) nell'ambito della *Strategia per l'Europa digitale* e del Piano d'azione per la democrazia europea presentati nel 2020 dalla Commissione europea (*Plasmare il futuro digitale dell'Europa*, Bruxelles, 19 febbraio 2020 COM(2020) 67 final e *Un'Europa pronta per l'era digitale: proposta della Commissione di nuove norme per le piattaforme digitali*, Bruxelles, 15 dicembre 2020) entrambi volti a regolare il «mercato unico digitale».

8. *Una Strategia europea per i dati*, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Bruxelles, 19 febbraio 2020, COM(2020)66 final.

9. Con riguardo alle norme tecniche, dalle quali potrebbe ricavarsi la terminologia alla quale fare ricorso per designare tali sistemi, è da rilevarsi che lo standard ISO relativo ai meccanismi di controllo dell'età (ISO/IEC 27566) è ancora in fase di sviluppo.

10. A tal proposito si vedano i relativi Considerando 47, 60 e gli artt. 12 e 27. La direttiva copre tutti i servizi con contenuti audiovisivi, indipendentemente dalla tecnologia utilizzata per fornire i contenuti. L'attuazione della direttiva in Italia si è avuta tramite l'adozione del d.lgs. 8 novembre 2021, n. 208 noto come Testo Unico sui Servizi Media Audiovisivi (TUSMA) che a tutela dei minori, agli articoli 41 e 42, prevede l'implementazione di meccanismi di limitazione all'accesso ai suddetti contenuti. A tal proposito v. OROFINO 2022.

11. Tale possibilità sembrerebbe potersi ricavare dal considerando 15 nonché dal n. 1, lett. a) dell'Allegato III all'AI Act.

di verifica dell'età basati su sistemi di identificazione digitale, in linea, a ben vedere, con gli studi finora condotti a livello europeo¹² e con le pratiche già in uso per l'attuazione del controllo parentale. Infine, con riferimento al contesto nazionale, in attuazione dell'obbligo di verifica dell'età previsto dal c.d. decreto Caivano (d.l. 15 settembre 2023, n. 123, convertito con modificazioni dalla legge 13 novembre 2023, n. 159)¹³, l'Autorità per le garanzie nelle comunicazioni (AGCOM), nella seduta del 24 settembre 2024, ha approvato lo schema di regolamento che disciplina le modalità tecniche e di processo per l'accertamento della maggiore età degli utenti, che vede come destinatari, ossia come soggetti regolamentati, i fornitori di servizi della società dell'informazione che diffondono contenuti a carattere pornografico¹⁴. Si tratta dunque di un intervento tanto urgente quanto settoriale riguardando lo stesso l'implementazione dei sistemi di controllo dell'età da parte solamente dei fornitori dei servizi digitali a contenuto pornografico.

L'avvento pervasivo delle tecnologie di intelligenza artificiale¹⁵, per loro natura 'dativore', sta accompagnando il fenomeno parallelo della repentina diffusione dei dispositivi *IoT*¹⁶. Sono plurimi i rischi che i minori ai quali sono esposti nell'ambiente digitale. Il minore, nell'accesso alle piattaforme online, può imbattersi in contenuti potenzialmente dannosi (es. violenti, pornografici, di disinformazione etc.) e può entrare in

contatto con un adulto potenzialmente pericoloso; può inoltre essere vittima o partecipare egli stesso a condotte pericolose tra pari d'età – quali il bullismo –, e nel firmare il contratto di adesione alla piattaforma (che comporta la cessione dei suoi dati) non ha consapevolezza dei rischi correlati.

Nonostante il mutamento sostanziale degli scenari, sia tecnologico sia giuridico, è da riconoscersi che il nucleo della disciplina di tali tecnologie si rinviene nel GDPR. È proprio l'assenza di una specifica previsione costituzionale dalla quale discende la possibilità di garantire al singolo il controllo sui propri dati e sui processi algoritmici che lo riguardano, che porta il giurista a ritenere disposizioni di rilievo *para-costituzionale* quelle discendenti dal GDPR. Il Regolamento costituisce il perno del diritto della società digitale, in quanto *strumentario normativo generale di livello para-costituzionale*¹⁷ concernente la tutela della persona con riguardo al trattamento dei propri dati personali. Non appare una mera circostanza il fatto che il GDPR e prima ancora il suo antecedente, costituito dalla Direttiva 95/46/CE, sono gli atti attorno ai quali si è formata la cultura giuridica europea e nazionale della protezione dei dati personali.

La disciplina prevista nel GDPR è improntata al principio del *favor minoris*¹⁸ in attuazione del *best interest of the child*¹⁹, sebbene nell'ambito

12. Tra i quali lo studio del Parlamento europeo, *Online age verification methods for children*, febbraio 2023 e il progetto euCONSENT (v. *supra* nota 3).

13. Art. 13-bis d.l. 123/2023.

14. Lo schema di regolamento si applica ai soli contenuti a carattere pornografico e dunque non a tutti i contenuti diffusi online. Nel comunicato stampa del 7 ottobre 2024 dell'AGCOM è affermato che le modalità tecniche adottate sono «altamente raccomandate con riferimento ad ulteriori tipologie di contenuti, oltre a quelli a carattere pornografico, che potrebbero comunque nuocere allo sviluppo fisico, mentale o morale dei minori».

15. Sulla necessità di una regolazione che non subordini mai la persona all'algoritmo e all'AI, bensì che identifichi in quest'ultima uno strumento al servizio dell'uomo v. PAPA 2022; COLAPIETRO 2023 e COLAPIETRO 2021.

16. Per gli aspetti critici legati alla profilazione sottesa al funzionamento di tali tecnologie v. PAPA 2020. I rischi online per i minori, come sopra indicati, sono stati classificati (LIVINGSTONE-STOILOVA 2021) con 4 C iniziali che normalmente vengono menzionate in inglese: *content, contact, conduct, contract* (contenuto, contatto, condotta e contratto).

17. IANNUZZI 2024, p. 24.

18. AGOSTINELLI 2023; BATTELLI 2022; BOMBILLAR SÁENZ 2018.

19. Perseguito sin dalla Convenzione sui diritti dell'infanzia e dell'adolescenza adottata nel 1989 dall'Assemblea Generale delle Nazioni Unite e ratificata dall'Italia nel 1991.

della tutela delle esigenze della circolazione dei dati. L'art. 24, par. 2 della Carta dei diritti fondamentali dell'UE, nota anche come Carta di Nizza²⁰, sancisce che «[i]n tutti gli atti relativi ai minori, siano essi compiuti da autorità pubbliche o da istituzioni private, l'interesse superiore del minore deve essere considerato preminente». Tale rilievo integra il carattere non assoluto che connota il trattamento dei dati personali, come ribadito nel Considerando 4 GDPR in base al quale «[i]l diritto alla protezione dei dati di carattere personale [...] va considerato alla luce della sua funzione sociale e va temperato con gli altri diritti fondamentali, in ossequio al principio di proporzionalità».

2. Alcuni chiarimenti definitivi: l'*age gate* e l'*age appropriate design*. La dimensione relazionale della tutela dei diritti del minore nella dimensione offline e in quella online

È opportuno dunque muovere da una precisazione terminologica concernente la dizione *age assurance* e il rapporto che intercorre con altre quali *age gate*, *age verification* o *age estimation* spesso impiegate in maniera equivalente. La specificità dell'esigenza di predisporre e pertanto di individuare le caratteristiche giuridiche dei sistemi di assicurazione dell'età deriva dalla necessità non solo di

verificare e dunque limitare l'accesso da parte dei minori ai più noti servizi della società dell'informazione, quali i social media, per loro vietati al di sotto dei 16 anni o comunque al di sopra dei 13 in base a quanto stabilito dagli Stati membri in osservanza dell'art. 8 par. 1 e 2 del GDPR (v. *infra* par. 2.1). Più in generale si tratta dell'esigenza di impedire l'accesso dei minori a contenuti per loro inappropriati, tra i quali – come visto – quelli pornografici o violenti o diretti alla vendita di alcol, tabacco, compreso il gioco d'azzardo, ecc.

In questo senso *age assurance* o assicurazione dell'età è un termine più ampio che si riferisce a qualsiasi sistema o processo progettato per garantire che gli utenti di un servizio online abbiano un'età appropriata per il contenuto o il servizio a cui stanno accedendo. I sistemi di verifica dell'età si collocano pertanto tra tali modalità di controllo classificabili sulla base di una scala di minore o maggiore attendibilità; a partire dall'autodichiarazione dell'età (riconosciuta a garanzia zero²¹), fino all'impiego di sistemi di riconoscimento biometrico che si avvalgono di algoritmi di intelligenza artificiale. In questo senso rileva inoltre l'esigenza di assicurare che la progettazione di servizi e prodotti digitali rispettino le esigenze e i diritti degli utenti in base alla loro età (*age appropriation design*)²². Un efficace sistema di *age verification*, infatti,

20. La Carta è stata firmata a Nizza nel dicembre 2000. L'articolo 6 del Trattato sull'UE, così come modificato dal Trattato di Lisbona, ha sancito la parificazione giuridica della Carta dei diritti fondamentali ai Trattati istitutivi dell'Unione.

21. Come rilevato nel provvedimento dell'Autorità garante per la protezione dei dati personali (provvedimento del 22 gennaio 2021, doc-web n. 9524194) con il quale è stata disposta la misura della limitazione dell'attività di trattamento dei dati relativi ai minori alla piattaforma *TikTok* per carenza delle misure adottate per la verifica dell'età degli iscritti. Il sistema previsto per la verifica dell'età consisteva nella mera indicazione da parte dello stesso utente.

22. Tale attenzione è presente quale azione chiave nell'ambito della strategia *Better Internet for Kids (BIK+)* tramite la quale la Commissione europea ha inteso sviluppare un codice di condotta sulla progettazione adeguata all'età (codice *BIK+*) che si baserà sul quadro normativo previsto dalla legge sui servizi digitali (DSA), contribuirà alla sua attuazione in linea con la direttiva AVMSD e il GDPR. Evidenze scientifiche relative all'impatto negativo dei social media sulla salute dei giovani, associato all'esposizione a contenuti non appropriati o dovuto ad un uso eccessivo, sono contenute negli avvisi del *Surgeon General* degli Stati Uniti del 2023 (CALZOLAI 2023). Risultanze non differenti si ricavano dal precedente studio *Young People's Mental Health in the Digital Age – Shaping the Future* condotto con riguardo ai Paesi europei dall'OCSE nel 2019. L'attenzione all'*age appropriation design* è presente anche nel *Children's Code* adottato nel 2019 dall'Information Commissioner's Office (Autorità garante per la protezione dei dati personali del Regno Unito), nel quale sono riportati i 15 standard che le piattaforme devono rispettare nel *best interest* dei minori. Tra questi è indicato l'*age appropriate application*, criterio che consiste nell'adottare un approccio basato sul rischio al fine di riconoscere l'età dei singoli utenti e assicurare l'applicazione in modo efficace degli altri standard del *Code*.

dovrebbe essere in grado di comunicare alla piattaforma, in maniera il più possibile analitica, in quale fascia di età si collocata l'utente, rendendo possibile proteggere gli utenti con riguardo non solo all'attuazione delle condizioni previste per l'accesso ma anche al trattamento dei contenuti relativi ai dati personali di questi ultimi²³.

Una tripartizione può inoltre rinvenirsi con riguardo al rischio crescente che deriva dall'impiego di tali processi in rapporto alla violazione delle istanze di tutela concernenti non solo la protezione dei dati personali ma anche la cybersecurity²⁴.

Costituiscono *species* o categorie di metodi di assicurazione dell'età, dunque, la mera autodichiarazione (*age gate*), sebbene giuridicamente non riconosciuta quale sistema per via della sua totale inefficacia²⁵, la verifica dell'età (*age verification*),

ma anche la stima dell'età (*age estimation*) che include una serie di misure e tecnologie diverse che solitamente ricorrono all'impiego di algoritmi di stima dell'età.

L'analisi appena condotta, invero, è funzionale a mettere in luce come la tutela del minore, declinata in rapporto alla protezione dei dati personali che lo riguardano nell'ambito dell'accesso ai servizi della società dell'informazione, si inserisce nella dimensione relazionale che caratterizza le molteplici tutele previste per il minore nello svolgimento della vita di relazione. Tale aspetto emerge fin dalla Convenzione sui diritti dell'infanzia e dell'adolescenza adottata nel 1989 dall'Assemblea Generale delle Nazioni Unite 1991, nonché con riguardo al nucleo dei principi costituzionali nazionali concernenti la dimensione offline della sua esistenza²⁶.

23. Spesso sono proprio le piattaforme a sollecitare i minori, in modo subliminale, a prestare il loro consenso digitale per aderire al servizio. Il Consiglio di Stato nelle sentenze del 29 marzo 2021, n. 2630 e n. 2631 ha ravvisato gli estremi della pratica ingannevole nella modalità di iscrizione al social network Facebook. Il servizio fornito dalla piattaforma veniva presentato come gratuito e non erano ben definite le finalità commerciali per le quali i dati dell'interessato sarebbero stati messi a disposizione.

24. Oltre agli studi richiamati in nota 3 si veda anche quanto rilevato dall'European Regulators Group for Audiovisual Media Services (ERGA) Subgroup 1 nel documento *Consistent implementation and enforcement of the European framework for audiovisual media services*, 2023. Sul rapporto tra cybersecurity e tutela dei dati personali v. PONTI 2024.

25. V. *postea* par. 3. Le soluzioni tecniche di verifica dell'età presenti sul mercato, tra le quali quelle realizzate da soggetti terzi che forniscono tali servizi, ad oggi sono le più disparate, e variano a seconda del servizio o bene cui il minore intende accedere. Per una rassegna dettagliata si v. EPRS, *Online age verification methods for children*, febbraio 2023.

26. L'interesse della società civile nei confronti dell'infanzia e dei minori ha cominciato a svilupparsi solo agli inizi del secolo scorso, soprattutto a livello internazionale. Per molto tempo, come avveniva nelle società arcaiche, quali quelle greca e romana, lo Stato si è occupato esclusivamente del cittadino, prevedendo per lo stesso tutele funzionali esclusivamente a tale status (PEPE 2019). Occorre inoltre tener conto che nell'era pre-digitale la funzione costruttiva dell'identità personale del figlio era prerogativa esclusiva dei genitori o della persona preposta dalla legge ad esercitare tutte o alcune delle funzioni genitoriali (GRISAFI 2024, p. 203). La dottrina italiana costituzionalistica da tempo ha manifestato attenzione per i diritti dei minori (v. PANUNZIO 1985). L'analisi dello stato giuridico del minore nel diritto costituzionale italiano deve prendere spunto dalla constatazione della relativa esiguità delle disposizioni contenute all'interno della Costituzione italiana che lo considerano non quale soggetto di diritti ma sempre in una dimensione di relazionalità. Il riferimento è agli artt. 30 e 31 Cost. – rispettivamente relativi al rapporto tra genitori e figli e alla tutela della gioventù da parte della Repubblica – che devono essere letti in combinato con gli artt. 2 e 3 Cost. Inoltre vi è l'art. 34 concernente il diritto all'istruzione (per il rapporto con la cultura digitale v. IANNUZZI 2009), l'art. 37 in materia di rapporti di lavoro e infine l'art. 48 con riguardo al diritto di voto che è implicitamente escluso per i minori. Il minore, quale soggetto debole, è pertanto tutelato in virtù dei doveri che ricadono sui genitori, pubblici poteri e in ultima analisi sull'intera collettività, al fine del corretto sviluppo della sua personalità. Si tratta di una impostazione non dissimile da quella adottata agli articoli 25 e 26 della Dichiarazione Universale dei Diritti dell'Uomo, adottata dall'Assemblea Generale delle Nazioni Unite il 10 dicembre 1948. Nonostante l'esiguità delle attenzioni rivolte al minore, la tutela costituzionale del medesimo non deve intendersi diminuita ma anzi deve essere intesa nella sua ampiezza,

Il quadro descritto, in questo senso, è da ricondursi all'affermazione del principio personalista cui è informata la Costituzione, che trova fondamento nell'art. 2. L'articolo 2 quale *norma-fondamento* del nostro ordinamento pone non solo i caratteri della forma di Stato («Repubblica» «riconosce e garantisce») ma anche una priorità di valore, esprimendo l'essenza del principio personalista («uomo» «come singolo») e pluralista («formazioni sociali») che verrà completato dal successivo art. 3, co. 2 Cost. Quest'ultimo nel sancire l'eguaglianza formale, integra la tutela formale da parte dello Stato con quella sostanziale, richiedendo l'intervento dei pubblici poteri per modificare o rimuovere le condizioni economiche e sociali che «impediscono il pieno sviluppo della persona umana»²⁷.

La dimensione relazionale in cui si trova il minore, che sottende dunque il rispetto per la sua libertà ma presuppone un dovere di solidarietà, caratterizza e fonda il rispetto per la sua autodeterminazione. Il principio personalista, difatti, indirizza l'azione del legislatore al pieno rispetto e sviluppo della persona, riportando al centro la sua autodeterminazione²⁸.

La tutela prevista con riguardo ai sistemi di verifica dell'età, riconosciuta ampiamente a livello

internazionale, costituisce anch'essa una tutela funzionale, in quanto rapportata precipuamente alla condizione di vulnerabilità del minore con riguardo all'ambiente online²⁹. Come si evince dal Considerando 38 GDPR, invero, i minori sono «meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali» e pertanto meritano una specifica protezione. La relazionalità quale dimensione di tutela prescelta per il minore si declina dunque sia contenutisticamente, con riguardo alle situazioni soggettive che fanno capo al medesimo, sia in senso procedurale, quale precipua modalità di tutela.

Con riguardo al contesto delle dinamiche relazionali ed economiche proprie della realtà digitale è innegabile che tale tutela debba attagliarsi al profilo circolatorio che caratterizza i dati del minore, parzialmente a scapito della garanzia della componente identitaria che pure, come visto, li contraddistingue. Il momento circolatorio connota il minore già quale fruitore dei servizi della società dell'informazione e dunque presuppone un bilanciamento tra diritti (v. *infra* par. 3.1).

derivante dal fatto che il minore, per il tramite della relazionalità, partecipa di tutti i diritti fondamentali che compongono i diritti di cittadinanza.

27. RUGGERI 2015, pp. 168 e 195 ss.; VEDASCHI 2011.

28. Sebbene nella Costituzione non vi sono riferimenti all'autodeterminazione in alcuna delle sue disposizioni, ciò in quanto l'autodeterminazione non era considerata una espressione giuridica, la giurisprudenza e la dottrina successive hanno contribuito a caratterizzarne la dimensione, non unitaria ma frammentata, in rapporto agli specifici aspetti delle scelte e decisioni individuali prese dall'individuo nell'ambito giuridico. A tal proposito v. MANGIAMELI 2009. La dimensione relazionale della tutela del minore viene valorizzata anche nelle pronunce della Corte costituzionale (tra le quali, Corte cost., sent. n. 79 del 2022 con commento di LAMARQUE 2023).

29. La tutela sovranazionale dei diritti e degli interessi delle persone di minore età è risalente. Con riguardo all'ambiente digitale il riferimento è al Commento generale n. 25 del 2021 sui diritti dei minorenni in relazione all'ambiente digitale, adottato dal Comitato delle Nazioni Unite sui Diritti dell'Infanzia e richiamato anche nel Considerando 9 dell'*AI Act*. Nell'ambito del capitolo dedicato alle Misure di protezione speciali e nello specifico in relazione alla protezione dallo sfruttamento economico, sessuale e di altro tipo è statuito (par. 114, p. 54) che «[g]li Stati parte dovrebbero [...] legiferare per garantire che i minorenni siano protetti da beni nocivi, come armi o droghe, o servizi nocivi, come il gioco d'azzardo. Dovrebbero poi essere utilizzati robusti sistemi di verifica dell'età per impedire ai minorenni di accedere a prodotti e servizi il cui possesso o utilizzo risultino illegali per loro. Tali sistemi dovrebbero essere coerenti con la protezione dei dati e con i pertinenti requisiti di salvaguardia». Tale esigenza era stata già individuata nel Commento generale n. 16 del 2013 del Comitato delle Nazioni Unite sui Diritti dell'Infanzia dedicato agli obblighi degli Stati relativamente all'impatto del settore delle imprese sui diritti dell'infanzia, così come nel Commento Generale n. 20 del 2016. Si segnala inoltre la Convenzione del Consiglio d'Europa sulla Protezione dei Bambini contro lo Sfruttamento e l'Abuso Sessuali, nota anche come Convenzione di Lanzarote, entrata in vigore il 1 luglio 2010.

3. I sistemi di assicurazione dell'età alla luce della finalità del trattamento. Il canone della proporzionalità sotteso alla verifica del c.d. consenso digitale

Prima che nel 2018 il GDPR entrasse in vigore in Europa non vi erano normative precise per il trattamento dei dati dei minori online. Il GDPR ha introdotto l'obbligo di verificare l'età, oltre che la prestazione o l'autorizzazione del consenso da parte degli esercenti la responsabilità genitoriale per l'accesso ai servizi della società dell'informazione (art. 8 GDPR)³⁰. L'art. 8, par. 1 GDPR dispone che ove il trattamento dei dati comuni preveda il consenso dell'interessato, se vi è «un'offerta diretta di servizi della società dell'informazione ai minori», tale trattamento «è lecito ove il minore abbia almeno 16 anni»; in caso di età inferiore va prestato o autorizzato da chi esercita la responsabilità genitoriale. Ai sensi dell'art. 8, par. 2 GDPR, ultimo capoverso, il limite di tale *maggior età digitale*³¹ o – se si vuole – *limitata capacità d'agire on-line*³² può venire ulteriormente abbassato dagli Stati nazionali ma non al di sotto dei 13 anni³³. L'età minima per esprimere il consenso al trattamento dei propri dati in Italia è stata portata dall'art. 2-*quinq*ues del d.lgs. 196/2003 (d'ora in poi, Codice privacy), adeguato dal d.lgs. 101/2018 al GDPR, a 14 anni, con la conseguenza che il minore di almeno 14

anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione; mentre il trattamento dei dati personali del minore di età inferiore a quattordici anni è lecito a condizione che il consenso sia prestato o autorizzato da chi esercita la responsabilità genitoriale³⁴.

Il rispetto dell'art. 8 GDPR comporterà innanzitutto per ogni fornitore di servizi in rete l'obbligo di verificare l'età del pubblico che intende fornire i dati personali alla sua organizzazione. Tale obbligo, stante l'assenza di una vera e propria declinazione delle caratteristiche tecniche che i titolari del trattamento devono implementare nello sviluppo dei sistemi di controllo dell'età, è soddisfatto tramite l'adozione di sistemi efficaci e non facilmente eludibili³⁵. All'obbligo, inoltre, è associata la necessità di adottare un meccanismo di blocco automatico dell'accesso ai contenuti qualora non sia rispettato il vincolo anagrafico.

Proprio l'adozione del principio della finalità del trattamento³⁶ – che costituisce presupposto per l'applicazione di tutti gli altri principi di liceità del trattamento, indicati all'art. 5 GDPR – consente di far emergere un primo limite posto a garanzia dei dati del minore, sottostante la verifica della maggiore età digitale ai fini della raccolta del consenso. Come ha affermato la dottrina, infatti, «la finalità

30. Nella Direttiva 95/46/CE non vi è alcun riferimento specifico né ai minori né ad altri soggetti privi della capacità d'agire. Tale scelta è coerente con la vigenza del Trattato di Maastricht che non conteneva alcuna disposizione che autorizzasse le istituzioni europee ad approvare norme nei settori dell'ordinamento civile e diritto della famiglia, di competenza degli Stati membri. Per tale ricostruzione v. OROFINO 2018, p. 9

31. AGOSTINELLI 2023.

32. RESTA 2022, pp. 105 ss.

33. Il par. 3 dell'art. 8 GDPR statuisce che quanto stabilito ai sensi del par. 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione e l'efficacia di un contratto rispetto a un minore.

34. Il ddl n. 1136 recante *Disposizioni per la tutela dei minori nella dimensione digitale*, intende (art. 3) innalzare la soglia dell'età per consenso digitale ad anni 15 per la valida conclusione dei contratti con i fornitori di servizi della società dell'informazione. Si noti invece come nel ddl n. 1146 *Disposizioni e delega al Governo in materia di intelligenza artificiale* è stabilito (art. 4) che l'accesso alle tecnologie di intelligenza artificiale è consentito ai maggiori di anni 14.

35. Provvedimenti n. 112 del 30 marzo 2023, doc-web. n. 9870832 e n. 114 dell'11 aprile 2023, doc-web n. 9874702 relativi al servizio *ChatGPT*; provv. n. 39 del 2 febbraio 2023, doc-web n. 9852214 relativo alla piattaforma *Replika*.

36. «I dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, paragrafo 1, considerato incompatibile con le finalità iniziali» (art. 5, par. 1, lett. b) GDPR).

del trattamento costituisce sempre misura della legittimazione e limite al trattamento dei dati personali»³⁷. L'indagine si soffermerà sull'applicazione della prima parte del suo enunciato, tralasciando, per ragioni di trattazione, gli aspetti legati al divieto di uso secondario dei dati personali.

Rileva, dunque, il primo corollario del principio, ossia la pertinenza, che si traduce nella legittimità del trattamento in rapporto allo scopo. La legittimità deve ritenersi integrata quale requisito generale sottostante allo scopo della verifica dell'età se è rispettato, in primo luogo, il canone della proporzionalità.

In tal senso la proporzionalità è da intendersi quale ragionevolezza. Lo strumento impiegato dovrà essere per quanto possibile meno invasivo con riguardo alla limitazione del controllo da parte del soggetto sui propri dati personali. Il titolare del trattamento è tenuto, in virtù degli obblighi di *accountability* (artt. 24 e 25 GDPR), a dimostrare di aver messo in atto le misure tecniche e organizzative adeguate al fine di effettuare il trattamento in modo conforme al GDPR. L'uso di metodi che rischiano di raccogliere dati concernenti l'attività online del minore (c.d. *age inference* o *data-intensive systems*) è a tal fine da ritenersi sproporzionata, con riguardo anche al rispetto del principio di minimizzazione. È pur vero che l'efficacia di tali controlli è fondamentale ai fini di una applicazione della previsione che non sia elusiva della legittimazione soggettiva. È utile notare che anche l'art. 28 DSA prevede che le piattaforme debbano

adottare misure «adeguate e proporzionate» al fine di garantire la protezione dei minori online. Tale criterio fonda, inoltre, anche la scelta della corretta base giuridica da parte del fornitore del servizio.

In secondo luogo, la proporzionalità si traduce nell'obbligo di fornire una adeguata informativa al minore che possa rendere il consenso prestato libero e consapevole in rapporto al servizio al quale il minore intende accedere³⁸. In base a quanto statuito dall'art. 12, n. 1 GDPR³⁹, come recepito dall'art. 2-*quinquies*, comma 2 del Codice privacy, a proposito di soggetti fragili, come i minori, l'informazione deve infatti essere resa accessibile, ossia deve essere redatto un prospetto informativo «conciso ed esaustivo, facilmente accessibile e comprensibile dal minore» (Considerando 58 GDPR). La dottrina non ha mancato di rilevare come la base giuridica del consenso presenti una insufficienza, nell'applicazione pratica in rapporto alla sottoscrizione dei servizi della società dell'informazione. Il consenso, infatti, non può intendersi quale espressione di vera e propria autodeterminazione, soprattutto in rapporto allo scambio tra dati dei minori e accesso ai servizi online⁴⁰.

3.1. Il bilanciamento tra diritti e il criterio di ragionevolezza: i cardini della disciplina delle nuove tecnologie. La sentenza della Corte costituzionale n. 69 del 2024

Si è detto che, stante un obbligo di verifica dell'età per i fornitori di servizi della società dell'informazione (art. 8 GDPR), a caratterizzare il quadro dei

37. PONTI 2023-A, p. 180.

38. Sull'informativa si veda quanto stabilito nel provv. n. 39 del 2 febbraio 2023 relativo alla piattaforma *Replika*.

39. A tal fine indicazioni, sebbene risalenti, si rinvencono nelle Linee guida sul consenso approvate dal WP29 il 10 aprile 2018 (WP259) e nelle Linee guida sul consenso ai sensi del regolamento (UE) 2016/679 adottate il 4 maggio 2020 dall'EDPB. Le prime contengono prescrizioni specifiche con riguardo ai social networks quali il non richiedere dati particolari nei moduli di iscrizione, la rinuncia al trattamento dei dati finalizzato al marketing diretto rivolto ai minori, l'acquisizione del preventivo consenso dei genitori etc. Le seconde forniscono maggiori chiarimenti relativamente all'espressione e alla correlata acquisizione di un consenso valido ai sensi di legge nei diversi settori in cui questo risulta rilevante ed utilizzabile. È espressamente previsto che il titolare del trattamento nel verificare la validità del consenso dal minore prestato è chiamato a «compiere ogni ragionevole sforzo per verificare che l'utente abbia raggiunto l'età del consenso digitale, e le misure dovrebbero essere proporzionate alla natura e ai rischi delle attività di trattamento» (p. 30). Inoltre è previsto che la «ragionevolezza degli sforzi, in termini di verifica tanto che l'utente abbia l'età sufficiente per esprimere il consenso quanto che la persona che esprime il consenso a nome del minore sia il titolare della responsabilità genitoriale, può dipendere dai rischi inerenti al trattamento e dalla tecnologia disponibile» (p. 31).

40. AGOSTINELLI 2023; BATTELLI 2022.

sistemi di controllo dell'età è la mancanza di una legge a contenuto tecnico-scientifico che ne individui le caratteristiche e contestualmente operi un bilanciamento tra esigenze contrapposte. Le nuove tecnologie hanno fatto emergere tuttavia come «in luogo dell'esaltazione della ragionevolezza scientifica la regolazione dovrà essere guidata da un giudizio di ragionevolezza, inteso come conciliazione di valori costituzionali nella sua accezione di canone di razionalità pratica»⁴¹.

Il tema del bilanciamento tra principi e diritti qui richiamato è centrale nella teoria dei diritti fondamentali nello stato costituzionale⁴². In tale paradigma è anche regolato il bilanciamento tra il diritto alla protezione dei dati personali e gli altri diritti costituzionali della persona. Da tale punto di vista, infatti, la sinergia multilivello tra previsioni normative e tutele giurisdizionali sta contribuendo alla costruzione di una precisa e nuova identità europea condivisa dagli Stati membri in materia⁴³.

A tal fine, per dare sostanza ai canoni del bilanciamento e della ragionevolezza, si ritiene opportuno avere riguardo alla tecnica del bilanciamento adottata dalla Corte costituzionale quale canone ermeneutico della Costituzione⁴⁴. Come è noto, i

metodi interpretativi della Costituzione sono plurimi. La fondamentale distinzione tra approccio interpretativo “normativo-formale” e “normativo-sostanziale”⁴⁵ è spiegabile proprio riprendendo una affermazione del giurista Zagrebelsky, il quale chiari in maniera emblematica che mentre la *ragione* esprime una misura di razionalità rispetto allo scopo, la *ragionevolezza* costituisce una misura di razionalità rispetto al valore⁴⁶.

Il criterio di ragionevolezza⁴⁷, insieme al metodo del bilanciamento⁴⁸, costituisce l'ingranaggio dell'interpretazione valoriale della Costituzione – cui, nella massima declinazione, è associata la teoria dell'art. 2 Cost. quale clausola aperta – che dà vita ad un processo nomofilattico a tutti gli effetti che non è lineare, come quello tradizionale legislativo, ma circolare.

Il riferimento ai criteri del bilanciamento e della ragionevolezza nell'operato della Corte costituzionale è dunque funzionale ai fini del proposito di individuare la miglior forma di regolazione per le tecnologie di verifica dell'età in quanto, come ha avuto modo di rilevare la Corte costituzionale⁴⁹, nonché emblematicamente la dottrina tedesca⁵⁰ già in tempi remoti, sebbene tutti i diritti, anche

41. IANNUZZI 2023, in partic. p. 101.

42. RIDOLA 2006.

43. Emblematico è il bilanciamento tra diritto alla tutela dei dati personali e diritto alla trasparenza. Con riguardo alla pronuncia Corte cost., sent. n. 20 del 2019 si v. PONTI 2019.

44. Vale rammentare come subito dopo l'entrata in vigore della Costituzione, prima che prendesse avvio il percorso di *costituzionalizzazione* della vita sociale (BALDASSARRE 2007), era invalsa una interpretazione della stessa al pari della legge ordinaria, sulla base dell'approccio giuspositivistico. Invero, fino alla metà del XX secolo il diritto è stato inteso quale *coazione*, ossia espressione dell'autorità pubblica, senza alcuno spazio per «le definizioni legali, i programmi, le determinazioni di fini, le promesse, gli auspici e soprattutto, i principi (scritti)» che venivano ritenuti contenuto non obbligatorio e per tale ragione non normativi e non rilevanti (BALDASSARRE 2007).

45. PACE 2003, p. 37.

46. PACE 2001, p. 59, il quale A. inoltre distingue la logica che presiede l'applicazione delle norme legislative ordinarie (“razionalità-rispetto-al-fine”) in contrapposizione alla logica che presiede l'applicazione delle norme costituzionali (“razionalità-rispetto-al-valore”). Si veda inoltre SCACCIA 2024, in partic. 63 ss.

47. Sul criterio di ragionevolezza si veda SCACCIA 2007.

48. SCACCIA 1998.

49. Si ricordi, fra tutte, Corte cost., sent. n. 85/2013 relativa al caso Ilva. In commento si v. ONIDA 2013, DIOTALLEVI 2014.

50. Per una ricostruzione storica del concetto di valore che «sconfinando dalla sua sfera originaria – l'economia – invade ogni ambito dell'esistenza sociale e politica» si vedano SCHMITT 1967/2008 e HARTMANN 1972 in partic. pp. 147-157. Sebbene l'ideologia personale propugnata da Hartmann si inserisca tra quelle antidemocratiche, come quella di Schmitt, è innegabile che la sua profonda riflessione sulla natura dei valori sia entrata nel dibattito dottrinale europeo.

costituzionali, tendono a dichiararsi assoluti, non esistono nell'ordinamento *diritti tiranni* che non debbano essere bilanciati con diritti e principi concorrenti⁵¹. Ciò vale in special modo per il diritto alla protezione dei dati personali la cui *costituzionalizzazione* a livello sovranazionale (si consideri anche il dato convenzionale, ossia l'art. 8 della CEDU) – come si è detto – è da sempre risultata decisiva in rapporto alla relativa tutela.

Un riflesso di tale implicito, e sempre sotteso bilanciamento tra protezione dei dati personali e altre istanze di tutela nella prospettiva multilivello, si rinviene anche nella recente sentenza n. 69 del 2024, con la quale la Corte costituzionale si è pronunciata sul riparto di competenza legislativa concernente la disciplina del trattamento dei dati personali⁵². La dichiarata incostituzionalità della disposizione della legge regionale della Regione Puglia che prevedeva ai fini dell'accreditamento delle strutture sociosanitarie l'installazione di sistemi di videosorveglianza quale forma di prevenzione di condotte di maltrattamento o di abuso in danno di persone vulnerabili, è specificamente circoscrivibile al riparto di competenza legislativa. Tuttavia, essa sottende la scelta, insita nel sistema multilivello di tutela della protezione dei dati personali, di valorizzare un nucleo irriducibile e condiviso tra gli Stati di tutela della persona in rapporto alla protezione dei propri dati personali.

Pertanto, sarà compito del legislatore statale, nell'ambito del margine di manovra che i regolamenti europei gli lasceranno, disciplinare la concreta attuazione di tali tecnologie avendo riguardo al fatto che i vincoli posti in Costituzione, come noto, operano essenzialmente in via negativa e pertanto nell'interpretazione degli stessi in rapporto alle nuove tecnologie di verifica dell'età egli dovrà averne riguardo.

4. Conclusioni. La sfida complessa di un'armonizzazione necessaria a livello europeo (GDPR, DSA) e nazionale

Dall'indagine svolta possono trarsi alcune riflessioni conclusive. In primo luogo, con riguardo alla frammentarietà che caratterizza il quadro normativo relativo agli obblighi di controllo dell'età. Si è detto che dall'art. 8 GDPR, che costituisce il fondamento della tutela del minore nella società digitale con riguardo all'accesso ai servizi della società dell'informazione, possono ricavarsi indicazioni solo parziali in termini di efficacia e ineludibilità per quanto attiene ai requisiti che il meccanismo di controllo dell'età deve avere, come attestano i plurimi provvedimenti adottati dall'Autorità garante per la protezione dei dati personali⁵³. Nonostante ciò, l'analisi condotta sulla base del principio della finalità del trattamento dei dati personali ha fatto emergere come la proporzionalità sia da ritenersi canone immanente all'applicazione della disposizione. Senz'altro tale aspetto permette di affermare che il recente e repentino sviluppo tecnologico al quale è sottesa l'imperante esigenza della circolazione dei dati – con parziale compressione dell'aspetto della protezione loro riconosciuta – sebbene (soprattutto in un primo momento) abbia messo a dura prova la graniticità della disposizione come attuata nei rispettivi ambiti nazionali, stia ora restituendo nuova centralità alla stessa. È innegabile che in tale processo un ruolo, non solo integrativo, è svolto dalle previsioni del DSA rivolte ai fornitori di piattaforme online e in special modo ai fornitori di piattaforme online «di dimensioni molto grandi» e di motori di ricerca online «di dimensioni molto grandi». Sebbene la concreta applicazione di entrambi gli artt. 28 e 35 è accompagnata dalla possibilità ancora non esercitata da parte della Commissione europea di emanare orientamenti sull'applicazione delle misure previste, ad oggi la cogenza delle misure è rimessa

51. BALDASSARRE 2007.

52. Anche nella precedente sent. n. 271 del 2005 la Consulta si era pronunciata sul riparto di competenza in materia. In commento v. FOÀ 2006.

53. V. *supra* par. 3, nonché si aggiungano i rilievi contenuti con riguardo ai processi di verifica dell'età nel provvedimento di avvertimento del GPDP del marzo 2024 relativo al protocollo privato citato in nota 4.

all'attuazione che ne viene data a livello nazionale con riguardo ad un dettato tutt'altro che chiaro⁵⁴.

Proprio in rapporto a tale livello, in secondo luogo, l'analisi condotta ha fatto emergere la necessità che venga implementata una cooperazione tra le Autorità nazionali designate a dare attuazione alle previsioni adottate in ambito europeo al fine di individuare le caratteristiche del sistema di verifica dell'età, non senza un previo bilanciamento tra il diritto alla protezione dei dati personali e la tutela del minore online. Tale bilanciamento finora è stato condotto in attuazione della previsione di cui all'art. 35 DSA con riguardo ai rischi associati alla pornografia minorile. Si tratta del modello di "prova dell'età" basato sul metodo denominato "della terza parte fidata", individuato, previa acquisizione del parere favorevole del Garante per la protezione dei dati personali, dall'AGCOM con provvedimento del settembre 2024 (v. *supra* par. 1), che è in attesa dell'ultimo vaglio della Commissione europea. Il processo di verifica dell'età è caratterizzato dall'indipendenza dal dispositivo di accesso o dal sistema operativo utilizzato dall'utente che intende fruire dei contenuti a carattere pornografico e dalla scelta per l'«approccio tecnologicamente neutrale» che lascia libertà di valutazione e scelta del sistema ai soggetti tenuti alla realizzazione dei processi di garanzia dell'età dell'utente.

Rimane tuttavia imperante l'esigenza, avvertita a livello nazionale⁵⁵, di implementare sistemi di assicurazione dell'età che proteggano il minore nei confronti di *qualsiasi* servizio della società dell'informazione, nel solco degli artt. 8 GDPR e 28 DGA, e non solo di quelli che forniscono l'accesso a contenuti a carattere pornografico. L'individuazione di standard di tutela comuni in tutti gli Stati membri costituisce il presupposto per addivenire ad un bilanciamento condiviso sottostante la scelta di un meccanismo di verifica dell'età che possa mitigare l'esigenza dell'attendibilità con i rischi per i dati personali – associati ad esempio alla profilazione o al trattamento di dati biometrici – nonché per la cybersicurezza. La mancanza di una regolamentazione e standardizzazione coerente nei diversi paesi può creare disparità e lacune con ricadute sull'efficacia delle soluzioni parzialmente adottate.

In virtù della forza espansiva della tutela dei dati personali, nel concreto bilanciamento tra diritti, occorre dunque ripartire da un'attuazione dell'art. 8 GDPR rispettosa del canone della ragionevolezza e da un intervento chiarificatore del dettato di cui all'art. 28 DSA. È senz'altro necessario un quadro di regole che, accompagnato a una educazione digitale⁵⁶, sappia coniugare la libertà del minore nella società digitale con l'invasività nella sfera della persona che viepiù caratterizza il mondo digitale⁵⁷.

54. Sebbene il par. 1 dell'art. 28 DGA prevede che «[i] fornitori di piattaforme online accessibili ai minori adottano misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori sul loro servizio», in base al successivo par. 3 «Il rispetto degli obblighi di cui al presente articolo non obbliga i fornitori di piattaforme online a trattare dati personali ulteriori per valutare se il destinatario del servizio sia minore». L'art. 28 deve dunque intendersi quale un obbligo di risultato non generalizzato a tutela dei minori (v. OROFINO 2024, p. 154).

55. Si tratta del ddl n. 1136 recante *Disposizioni per la tutela dei minori nella dimensione digitale* tramite il quale si vorrebbe introdurre un obbligo generalizzato di verifica dell'età (art. 2) per ciascun fornitore di servizi della società dell'informazione che diffonde i propri servizi in Italia sulla base delle modalità tecniche e di processo stabilite dall'AGCOM di concerto con l'Autorità garante per la protezione dei dati personali. Dalla XIV edizione dell'Atlante dell'infanzia a rischio in Italia 2023 "Tempi digitali", elaborato su dati ISTAT rilevati a livello nazionale riferiti al 2022, si evince un drastico abbassamento dell'età in cui i minori e i pre-adolescenti (11-13 anni) accedono ai servizi online.

56. È inoltre necessaria «un'educazione digitale che permetta di interpretare criticamente gli elementi informativi e comunicativi, che sia coerente con i principi e valori che sostengono la democrazia e che risulti efficace al fine di realizzare l'obiettivo fondamentale di una formazione libera e piena della personalità dei discenti. Per questa ragione, risulta fondamentale garantire in modo permanente la presenza di abilità, in generale, ai fini dell'utilizzo delle TIC con misure di protezione e senza intrusioni, affrontando altresì le falle dell'uguaglianza e di genere che notoriamente sono sorte a causa di diversi fattori» (CÁMARA VILLAR 2023).

57. RODOTÀ 1997; con riguardo alle ricadute sull'identità, si v. RODOTÀ 2012, p. 334 ss.

Riferimenti bibliografici

- B. AGOSTINELLI (2023), *Minori in rete: l'illusione del consenso e l'equivoco della privacy*, in "Familia", 2023, n. 3
- A. BALDASSARRE (2007), *Interpretazione e argomentazione nel diritto costituzionale*, in "costituzionalismo.it", 2007, n. 2
- E. BATTELLI (2022), *Il trattamento dei dati nel prisma della tutela della persona minore di età*, in "Il Diritto dell'informazione e dell'informatica", 2022, n. 2
- F.M. BOMBILLAR SÁENZ (2018), *Protección y tutela de los derechos fundamentales del menor como sujeto activo y pasivo de los contenidos audiovisuales*, in F.J. Durán Ruiz (dir.), "Desafíos de la protección de menores en la sociedad digital: Internet, redes sociales y comunicación", Tirant lo Blanch, 2018
- S. CALZOLAIO (2023), *Social media e minori. Il Safety-first approach. Nota a: U.S. Surgeon General, Social Media and Youth Mental Health. The U.S. Surgeon General's Advisory*, in "Rivista italiana di informatica e diritto", 2023, n. 2
- G. CÁMARA VILLAR (2023), *Diritto all'educazione, pluralismo e società aperta nell'era digitale*, in "Iceonline.eu", 2023, n. 2 sp.
- E. CARLONI (2015), *Tendenze recenti e nuovi principi della digitalizzazione pubblica*, in "Giornale di diritto amministrativo", 2015, n. 2
- C. COLAPIETRO (2023), *Gli algoritmi tra trasparenza e protezione dei dati personali*, in "federalismi.it", 2023, n. 5
- C. COLAPIETRO (2021), *The impact of information and technology revolution on the constitutional rights with particular attention to personal data protection issues*, in M. Belov (ed.), "Information and Technology Revolution and its impact on State, Constitutionalism and Constitutional Law", Hart Publishing, 2021
- G. DIOTALLEVI (2014), *La crisi finanziaria europea e i diritti dei cittadini*, in "Questione Giustizia", 2014, n. 1
- M. FALCONE (2023), *Ripensare il potere conoscitivo pubblico tra algoritmi e Big Data*, Editoriale Scientifica, 2023
- S. FOÀ (2006), *Tutela della privacy e sistemi informativi regionali: il potere normativo regionale è riconosciuto solo se richiama e rispetta il codice sul trattamento dei dati personali*, in "federalismi.it", 2006, n. 3
- R. GRISAFI (2024), *Il dovere di educazione digitale tra sviluppo dell'identità del minore e responsabilità genitoriale*, in A. Morace Pinelli (a cura di), "Riflessioni sul diritto di famiglia effettivo. Continuando a dialogare con Cesare Massimo Bianca", Pacini Giuridica, 2024
- N. HARTMANN (1972), *Introduzione all'ontologia critica*, Guida, 1972
- A. IANNUZZI (2024), *Le fonti del diritto dell'Unione europea per la disciplina della società digitale*, in F. Pizzetti (a cura di), "La regolazione europea della società digitale", Giappichelli, 2024
- A. IANNUZZI (2023), *Paradigmi normativi per la disciplina della tecnologia: auto-regolazione, co-regolazione ed etero-regolazione*, in "Bilancio Comunità Persona", 2023, n. 2
- A. IANNUZZI (2009), *Diritto all'istruzione e cultura digitale*, in "Informatica e diritto", 2009, n. 2
- E. LAMARQUE (2023), *Diritti fondamentali della persona di minore età e best interests of the child*, in "www.giustiziainsieme.it", 2023
- S. LIVINGSTONE, M. STOILOVA (2021), *The 4Cs: Classifying Online Risk to Children*, CO:RE Short Report Series on Key Topics, 2021

- S. MANGIAMELI (2009), *Autodeterminazione: diritto di spessore costituzionale?*, in Id. (a cura di), "Teoria del diritto e dello Stato", Aracne, 2009
- V. ONIDA (2013), *Un conflitto fra poteri sotto la veste di questione di costituzionalità: amministrazione e giurisdizione per la tutela dell'ambiente. Nota a Corte costituzionale, sentenza n. 85 del 2013*, in "Rivista AIC", 2013, n. 3
- M. OROFINO (2024), *Il Digital Service Act tra continuità (solo apparente) ed innovazione*, in F. Pizzetti (a cura di), "La regolazione europea della società digitale", Giappichelli, 2024
- M. OROFINO (2022), *La normativa a tutela dei minori nel Testo Unico per la fornitura di servizi di media audiovisivi con uno sguardo rivolto al regolamento (UE) 2022/2065*, in "MediaLaws", 2022, n. 3
- M. OROFINO (2018), *Minori e diritto alla protezione dei dati personali*, in M. Orofino, F.G. Pizzetti (a cura di), "Privacy, minori e cyberbullismo", Giappichelli, 2018
- A. PACE (2003), *Problematica delle libertà costituzionali. Parte generale*, Cedam, 2003
- A. PACE (2001), *Metodi interpretativi e costituzionalismo*, in "Quaderni costituzionali", 2001, n. 1
- S.P. PANUNZIO (1985), *Premesse per uno studio sui diritti costituzionali e la capacità dei minori*, in Aa.Vv., "Scritti in onore di Vezio Crisafulli", vol. II, Cedam, 1985
- A. PAPA (2022), *Intelligenza Artificiale e decisioni pubbliche tra tecnica, politica e tutela dei diritti*, in "federalismi.it", 2022, n. 22
- A. PAPA (2020), *La complessa individuazione di un "equo" bilanciamento tra tutela della privacy e profilazione della big data society*, in V. Falce (a cura di), "Fairness e innovazioni nel mercato digitale", Giappichelli, 2020
- L. PEPE (2019), *I minori e il diritto in Grecia e a Roma*, in C. Lambrugo (a cura di), "Una favola breve. Archeologia e antropologia per la storia dell'infanzia", All'Insegna del Giglio, 2019
- B. PONTI (2024), *Il rapporto tra cybersicurezza e tutela dei dati personali: sinergie, bilanciamenti e parallelismi*, in "Rivista italiana di informatica e diritto", 2024, n. 2
- B. PONTI (2023-A), *Attività amministrativa e trattamento dei dati personali. Gli standard di legalità tra tutela e funzionalità*, FrancoAngeli, 2023
- B. PONTI (2023-B), *Tre scenari di digitalizzazione amministrativa "complessa": dalla interoperabilità predicata alla standardizzazione praticata*, in "Istituzioni del federalismo", 2023, n. 3
- B. PONTI (2019), *Il luogo adatto dove bilanciare. Il "posizionamento" del diritto alla riservatezza e alla tutela dei dati personali vs il diritto alla trasparenza nella sentenza n. 20/2019*, in "Istituzioni del federalismo", 2019, n. 2
- F. RESTA (2022), *Sub art. 8 GDPR*, in G.M. Riccio, G. Scorza, E. Belisario (a cura di), "GDPR e normativa privacy. Commentario", Ipsoa, 2022
- P. RIDOLA (2006), *Diritti fondamentali. Un'introduzione*, Giappichelli, 2006
- S. RODOTÀ (2012), *Il diritto di avere diritti*, Laterza, 2012
- S. RODOTÀ (1997), *Tecnopolitica: la democrazia e le nuove tecnologie della comunicazione*, Laterza, 1997
- A. RUGGERI (2015), *Il principio personalista e le sue proiezioni*, in L. Ventura, A. Morelli (a cura di), "Principi costituzionali", Giuffrè, 2015
- G. SCACCIA (2024), *Diritti fondamentali, legislazione e giurisdizione. Scritti scelti*, Edizioni Scientifiche Italiane, 2024

- G. SCACCIA (2007), *Controllo di ragionevolezza delle leggi e applicazione della Costituzione*, in A. Cerri (a cura di), "La ragionevolezza nella ricerca scientifica e il suo ruolo specifico nel sapere giuridico", Aracne, 2007
- G. SCACCIA (1998), *Il bilanciamento degli interessi come tecnica di controllo costituzionale*, in "Giurisprudenza costituzionale", 1998, n. 6
- C. SCHMITT (1967/2008), *Die Tyrannei der Werte*, Kohlhammer, 1967, trad. it. *La tirannia dei valori. Riflessioni di un giurista sulla filosofia dei valori*, Adelphi, 2008
- UNITED NATIONS SAFE ONLINE (2024), [*Feasibility Study for AVP Interoperability between Native Mobile Applications - EuConsent*](#), 2 February 2024
- A. VEDASCHI (2013), *Il principio personalista*, in L. Mezzetti (a cura di), "Diritti e doveri", Giappichelli, 2013



FRANCESCA RICCIULLI

L'identità e l'identificazione digitale del minore tra normativa nazionale e internazionale e i provvedimenti delle autorità competenti

Il contributo, prendendo le mosse dallo schema di regolamento licenziato dall'AGCOM all'esito della consultazione sugli strumenti di *age assurance* avviata in attuazione del c.d. "Decreto Caivano", si propone di analizzare i futuri scenari normativi e applicativi relativi agli strumenti di identificazione e autenticazione dei minori. In particolare, si esamineranno gli strumenti attualmente previsti dalla normativa italiana, che stabilisce requisiti specifici per l'identificazione degli utenti, e le intersezioni di questi ultimi con le disposizioni da ultimo previste dal regolamento europeo c.d. "eIDAS 2", il quale si prefigge di garantire un'identità digitale sicura e interoperabile a livello europeo. Ciò al fine di approfondire opportunità e criticità poste dalle scelte effettuate dalla governance.

*Identità – Identità digitale – Minori – Portafoglio digitale – Strumenti di identificazione – Verifica dell'età
Servizi digitali*

The identity and digital identification of minors between national and international regulations and the measures of the competent authorities

This contribution, starting from the draft regulation approved by AGCOM following the consultation on age assurance tools initiated in implementation of the so-called "Caivano Decree", aims to analyze future regulatory and applicative scenarios related to the identification and authentication tools for minors. In particular, it will examine the tools currently provided for by Italian legislation, which establishes specific requirements for user identification, and the intersections of these with the provisions recently outlined in the European regulation known as "eIDAS 2", which aims to ensure a secure and interoperable digital identity at the European level. The goal is to explore the opportunities and challenges posed by the governance's choices.

Identity – Digital identity – Minors – Digital wallet – Identification tools – Age verification – Digital services

L'Autrice è dottoranda in Diritto pubblico presso l'Università degli Studi Roma Tre

Questo contributo fa parte della sezione monografica *Minori e Internet* a cura di Carlo Colapietro e Antonio Iannuzzi

SOMMARIO: 1. L'identità digitale del minore e la fruizione dei servizi online. – 2. L'evoluzione dell'identità digitale nella normativa italiana. – 3. SPID per i minori: le Linee guida dell'Agenzia per l'Italia digitale. – 4. Le più recenti novità della normativa in materia di *age verification* in Europa. – 5. I principi affermati da AGCOM sui metodi di *age assurance*. – 6. Prime conclusioni.

1. L'identità digitale del minore e la fruizione dei servizi online

Negli ultimi anni, il dibattito sull'opportunità di rafforzare la tutela dei minori nel contesto digitale è diventato sempre più rilevante, alla luce dell'integrazione crescente delle tecnologie digitali nella vita quotidiana dei giovani, che si trovano sempre più frequentemente a vivere in una dimensione digitale e a fruire di servizi online¹.

Il presente contributo vuole soffermarsi, in particolare, sull'identità digitale del minore e sulla sua identificazione, alla luce del decreto legge c.d. "Caivano"² e dello schema di regolamento adottato successivamente dall'AGCOM³.

Non può parlarsi di identità digitale del minore senza soffermarsi brevemente sui temi dell'"identità" e dell'"identità personale", nonché sulla accezione loro storicamente attribuita in ambito giuridico.

Il significato della parola "identità" si evoluto in modo sorprendente con il passare degli anni, divenendo sempre più multiforme e, a tratti, inafferrabile⁴.

Ciò, anzitutto, per quanto riguarda il concetto stesso di "identità" – individuale, di gruppo, collettiva, sociale o nazionale – e le sue modalità di formazione⁵. Va aggiunto, poi, che non solo esistono diversi tipi di identità ma anche varie dimensioni della stessa, in quanto deve essere considerato sia come una persona crede di essere che come vuole essere rappresentata, oltre a come viene rappresentata dagli altri⁶. Si aggiunge, poi, che ciascun individuo non ha una sola identità definita e stabile ma, come è stato rilevato dai più, in ciascuna persona convivono più identità⁷.

Proprio tale ultima circostanza deve essere considerata con particolare riferimento al tema in

1. Sulla tutela del minore, con particolare riferimento al contesto digitale, v. BATTELLI 2021. V. anche: STANZIONE 2014; DI SABATO 2011; STANZIONE-SCIANCALEPORE 2006.

2. d.l. 15 settembre 2023, n. 123, convertito con modificazioni dalla l. 13 novembre 2023, n. 159 (in G.U. 14 novembre 2023, n. 266).

3. Schema di provvedimento su modalità tecniche e di processo per l'accertamento della maggiore età degli utenti approvato dal Consiglio in data 24 ottobre 2024 e, al momento in cui si scrive, notificato alla Commissione europea ai sensi della Direttiva (UE) 2015/1535.

4. Per una ricostruzione storica approfondita cfr. ALPA 2021. L'autore afferma condivisibilmente che, «a differenza di quanto accadeva in passato, l'"identità personale" è diventata un'espressione polisensa e con molti margini di ambiguità». E, ancora, che «identità dunque è una parola con molti significati e per sua natura misteriosa e ambigua: attraversa i secoli portando con sé il bagaglio onusto del passato, si riflette nel presente e si proietta nel futuro»; v. anche GLEASON 1983.

5. Cfr., tra gli altri, HETERINGTON 1998.

6. RICCA 2008.

7. PINO 2010; FRIEDMAN 2002.

oggetto, poiché nel minore possono, in effetti, coesistere molteplici identità, riflesso della sua complessità interiore, e al contempo egli sviluppa nuove identità nel corso della sua crescita, adattandosi e trasformandosi in risposta alle esperienze e alle fasi evolutive che attraversa. In questo senso, la letteratura e la normativa si riferiscono al minore, parlando indifferentemente di “infanzia”, “adolescenza”, “gioinezza”, “fanciullo”, senza riuscire, spesso, ad afferrare la complessità di tale soggetto, che cresce e muta molto velocemente. Si potrebbe rilevare che ogni individuo cresce e si evolve incessantemente, ma deve considerarsi che la tutela del minore di età è, in linea generale, rafforzata e specifica in ragione di una sua presunta o effettiva maggiore “fragilità”⁸.

Da un punto di vista strettamente giuridico, come rilevato da vari autori, nel testo della Costituzione si rinviene più volte il termine “persona” ma è del tutto assente qualsiasi riferimento al termine “identità” o alla stessa associata ad attributi come “individuale” o “personale”⁹.

Nell’ambito della normativa di rango primario, invece, il concetto di identità personale si rinviene

prima nella legge n. 675 del 1996¹⁰ e, successivamente, nel d.lgs. n. 196 del 2003¹¹, ora modificato dal decreto legislativo n. 101 del 2018, che ha adeguato la normativa nazionale alle disposizioni del Regolamento generale per la protezione dei dati personali n. 2016/679 dell’Unione europea (c.d. “RGPD o in inglese “GDPR”). Si tratta di entrambi testi normativi relativi alla protezione dei dati personali.

Storicamente, in effetti, l’elaborazione della nozione giuridica di “identità personale” non si deve alle codificazioni ma alla dottrina e alla giurisprudenza che si sono sviluppate già in tempi più risalenti sul tema¹². In particolare, si sono sviluppate due nozioni di identità personale, una c.d. “estrinseca” e una “sostanziale”¹³. Quest’ultima è stata ricostruita in una prima frase come “diritto ad essere correttamente rappresentati”¹⁴, in una seconda, a partire dalla storica sentenza della Corte costituzionale del 1994, come “diritto ad essere sé stessi”¹⁵.

La nozione che viene in rilievo in questa sede, però, è la prima, cioè quella di identità c.d.

8. Si pensi, ad esempio, all’art. 61 c.p., che disciplina le circostanze aggravanti comuni, ovvero quelle situazioni al verificarsi delle quali il giudicante deve aumentare la pena finale da infliggere al reo. Ebbene, l’art. 61 n. 5 c.p. disciplina l’aggravante della minorata difesa, che ricorre ogniqualvolta l’autore del reato approfitta di «circostanze di tempo, di luogo o di persona, anche in riferimento all’età, tali da ostacolare la pubblica o privata difesa». Trattasi, pertanto, della situazione di colui che, per un qualunque motivo, si trova in una peculiare situazione di debolezza e/o inferiorità rispetto a colui che pone in essere la condotta delittuosa. Si noti anche che la “fragilità”, in questo, come in altri casi, può essere dovuta anche all’età molto avanzata.

9. Tra gli altri cfr. MORELLI 2019. Tale circostanza sarebbe da imputare al fatto che il peso dell’esperienza autoritaria, che rappresentò, in negativo, un punto di riferimento costante per i Costituenti sia per l’elaborazione della parte della Carta relativa ai diritti sia per quella concernente i poteri, evidentemente dissuase gli autori del testo dall’introdurre riferimenti espliciti all’idea di un’identità collettiva, eccetto i richiami al concetto di “nazione”.

10. Cfr. art. 1: «La presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all’identità personale; garantisce altresì i diritti delle persone giuridiche e di ogni altro ente o associazione», successivamente abrogato ai sensi dell’articolo 183, comma 1, lettera a), del Codice in materia dei dati personali.

11. Cfr. art. 2: «Il presente testo unico, di seguito denominato “codice”, garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell’interessato, con particolare riferimento alla riservatezza, all’identità personale e al diritto alla protezione dei dati personali».

12. Per un approfondimento sul tema del diritto all’identità personale da un punto di vista storico e con riferimento ad entrambe le prospettive cfr. PINO 2010. Cfr. anche PINO 2003; TRUCCO 2004; RANDAZZO 2021; RAFFIOTTA 2010; RESTA 2007.

13. PINO 2010.

14. Lettura della prima dottrina: DE CUPIS 1949; ASCARELLI 1957; ARE 1965 e della prima giurisprudenza: Pretura di Roma del 6 maggio 1974 ma anche la nota Corte Cass n. 3769 del 22 giugno 1985.

15. Corte Cost. sent. n. 13 del 1994.

“estrinseca”, intesa come mezzo che consente l'identificazione di un soggetto¹⁶, in quanto più legata alla identità digitale¹⁷ e all'oggetto del presente contributo.

Questa nozione dell'identità personale è, a ben vedere, la ricostruzione più tradizionale ed è stata definita dalla dottrina più recente anche “anagrafica”¹⁸, in quanto si riferisce al complesso delle risultanze anagrafiche che servono a identificare il soggetto nei suoi rapporti con i poteri pubblici e a distinguerlo dagli altri consociati¹⁹ e si rinviene anche in alcune codificazioni più risalenti²⁰.

È evidente che il tema riguarda ogni individuo, non solo i minori. L'identificazione delle persone all'interno della società, del resto, persegue un fine prima di tutto pubblicistico, regolando i rapporti tra i cittadini e lo Stato²¹. Più nel dettaglio, consente allo Stato di esercitare un controllo sul territorio e sulla popolazione, tanto per finalità di sicurezza quanto per la efficace e efficiente organizzazione dei servizi amministrativi. Tale controllo si riflette altresì nell'ambito del diritto privato, dove la precisa identificazione assume il ruolo di garanzia dei rapporti tra i consociati.

2. L'evoluzione dell'identità digitale nella normativa italiana

L'identità digitale avrebbe, secondo alcuni, la stessa natura bifronte dell'identità personale, potendo

essere intesa, in modo più sostanziale, come *alter ego* virtuale della persona²² oppure, in una nozione più tecnica, come insieme delle informazioni che di una persona consentono l'identificazione²³.

Da un punto di vista squisitamente giuridico, il concetto di “identità digitale” o “identità elettronica” è stato codificato, a livello nazionale, all'interno del d.lgs n. 82 del 2005, recante il “Codice dell'amministrazione digitale” (noto anche come “CAD”), testo di riferimento per la normativa in materia di trasformazione digitale della pubblica amministrazione.

Ai fini del presente contributo, può essere utile una precisazione proprio sull'ambito soggettivo del d.lgs n. 82 del 2005.

Se la versione originaria del Codice ne limitava l'ambito di applicazione solo alle pubbliche amministrazioni di cui all'art. 1, comma 2, d.lgs. n. 165/2001 e alle società ed enti inseriti nel conto economico consolidato dello stato (redatto da Istat), a seguito del d.lgs. n. 179/2016 e d.lgs. n. 217/2017, è stato novellato l'art. 2, comma 2 del Codice, prevedendo che le disposizioni in esso contenute si applichino, oltre alle pubbliche amministrazioni in senso stretto (art. 2, comma 2, lett. a)), anche:

b) ai gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse²⁴; e

16. FINOCCHIARO 2010. Sulla individuazione “inequivoca” della persona v. RESTA 2007.

17. Per un approfondimento cfr. RICCIULLI 2024.

18. PINO 2010. Come affermato dall'autore, in questo senso, il rilievo giuridico dell'identità personale consiste nell'insieme dei segni distintivi esteriori della persona: il nome, alcune caratteristiche somatiche (l'altezza, il sesso), l'indirizzo di residenza – in ciò che può rendere quella persona facilmente identificabile da parte del pubblico potere.

19. cfr. RESTA 2007; BASSU 2021.

20. Sull'identificazione da parte del notaio v., ad esempio, l'art. 49, l. 89/1913.

21. Cfr. TRUCCO 2004.

22. In questo senso, IANNUZZI-LAVIOLA 2023, p. 12.

23. In questo senso, v. RESTA 2007. Per un approfondimento sul tema cfr. anche LUCIANI 2018; ALPA 2021.

24. Si riporta quanto contenuto nella Relazione illustrativa allo schema di decreto legislativo di attuazione della legge n. 124/2015 (recante “Deleghe al Governo in materia di riorganizzazione delle pubbliche amministrazioni”), nella quale si chiarisce che è stato previsto un elenco dettagliato di soggetti a cui si applicano le norme del CAD, specificando che «per i gestori di servizi pubblici ciò avviene in relazione ai servizi di pubblico interesse. Tenuto conto del grande numero di servizi pubblici forniti da soggetti privati in forza di concessioni, infatti, si è ritenuto opportuno riconoscere agli utenti analoghi diritti di cittadinanza digitale anche in relazione ai fornitori di detti servizi, in attuazione di quanto previsto dal principio di delega contenuto nell'articolo 1, comma 1, lettera h) ai sensi del quale tra gli obiettivi dell'intervento normativo vi è anche quello di semplificare le condizioni di

c) alle società a controllo pubblico, come definite nel d.lgs. 175/2016, escluse le società quotate di cui all'articolo 2, comma 1, lett. p), del medesimo decreto che non rientrino nella lettera b)²⁵.

Con riferimento alla *ratio* della novella legislativa, si ritiene che debba essere rinvenuta, oltre che nell'evitare sprechi di risorse pubbliche, nell'intento del Legislatore di rafforzare il riconoscimento dei diritti digitali dei cittadini e degli utenti, estendendo, a tal fine, il campo soggettivo di applicazione del Codice.

In tal senso, si ritiene utile ricordare che la Relazione illustrativa allo schema di decreto legislativo di attuazione della richiamata l. n. 124/2015 fissa come obiettivo principale dell'intervento normativo la semplificazione dell'esercizio dei diritti del cittadino, in materia di digitalizzazione, favorendo servizi per la collettività sicuri, accessibili, interoperabili e trasparenti. Si spiega, dunque, il perché sia stato previsto un ampliamento della platea dei soggetti, che a qualunque titolo e costituiti in qualsiasi forma giuridica, svolgono un servizio di pubblico interesse: il diritto ad un servizio pubblico qualitativamente alto, al quale il cittadino può partecipare direttamente e del quale ha diritto a rimanere soddisfatto.

Per completezza, risulta utile aggiungere che il comma 3 dell'art. 2 CAD specifica che «con riferimento al documento informatico, alle firme elettroniche e ai servizi fiduciari di cui al Capo II, alla

riproduzione e conservazione dei documenti di cui agli articoli 43 e 44, al domicilio digitale e alle comunicazioni elettroniche di cui all'articolo 3-bis e al Capo IV, all'identità digitale di cui agli articoli 3-bis e 64, le disposizioni del Codice e le relative Linee guida concernenti si applicano anche ai privati, ove non diversamente previsto».

Gli articoli da 3 a 9 di questo Codice dell'amministrazione digitale formano la «Carta della cittadinanza digitale», sezione che prevede un nucleo minimo di diritti e doveri digitali degli «utenti» e che questi ultimi vantano nei confronti dei soggetti citati obbligati all'applicazione del Codice²⁶.

Diritto fondamentale previsto dalla Carta della cittadinanza digitale è il diritto all'identità digitale, regolato dall'art. 3-bis CAD²⁷. La disposizione prevede il diritto di chiunque di accedere ai servizi online dei soggetti di cui all'art. 2, comma 2 CAD, utilizzando un sistema di identificazione elettronica, come lo SPID (Sistema Pubblico di Identità Digitale)²⁸ o la Carta di Identità Elettronica (CIE), nonché tramite la c.d. «app IO» (punto di accesso telematico di cui all'art. 64-bis CAD).

L'art. 7 CAD, dedicato ai servizi online, dal canto suo, prevede l'obbligo per i soggetti di cui all'art. 2, comma 2 CAD di consentire l'accesso ai propri servizi tramite il proprio sito a valle, se occorre, di identificazione tramite gli strumenti menzionati, oppure tramite il punto di accesso telematico di cui all'art. 64-bis CAD (c.d. «app IO»)²⁹.

esercizio dei diritti e l'accesso ai servizi di interesse dei cittadini, obiettivo che si persegue ampliando il novero dei soggetti tenuti ad applicare le norme del CAD».

25. Con riguardo alla lettera c), pur non essendo particolarmente critica l'interpretazione circa i soggetti individuati dalla disposizione, vista la chiara definizione di società a controllo pubblico, quali «società in cui una o più amministrazioni pubbliche esercitano poteri di controllo», più problematica risulta l'esclusione delle società quotate, come definite all'articolo 2, comma 1 del d.lgs. 175/2016. Il CAD, infatti, esclude le società quotate dall'applicazione del testo, ma solo se le medesime società non siano gestori di servizi pubblici e non esercitino servizi di pubblico interesse.
26. Ad eccezione di casi specifici, di solito tutti i soggetti di cui all'art. 2, comma 2 CAD.
27. Art. 3-bis CAD, rubricato «Identità digitale e Domicilio digitale», al comma 01, afferma che «Chiunque ha il diritto di accedere ai servizi on-line offerti dai soggetti di cui all'articolo 2, comma 2, tramite la propria identità digitale e anche attraverso il punto di accesso telematico di cui all'articolo 64-bis».
28. «Insieme aperto di soggetti pubblici e privati» che, previo accreditamento da parte dell'AgID, «identificano gli utenti per consentire loro il compimento di attività e l'accesso ai servizi in rete» (cfr. art. 64, comma 2-ter, CAD). Sistema istituito dall'art. 17-ter d.l. 21 giugno 2013, n. 69 (conv. con mod. dalla legge 9 agosto 2013, n. 98), di modifica dell'art. 64 del d.lgs. n. 82/2005, al fine di «favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese» (cfr. art. 64, comma 2-bis, CAD).
29. Art. 7 CAD, rubricato «Diritto a servizi on-line semplici e integrati» afferma che: «1. Chiunque ha diritto di fruire dei servizi erogati dai soggetti di cui all'articolo 2, comma 2, in forma digitale e in modo integrato, tramite

Con specifico riferimento a SPID, il d.P.C.M. del 24 ottobre del 2014 ha definito l'identità digitale come "la corrispondenza biunivoca tra un utente e i suoi attributi identificativi, certificata attraverso dati raccolti e registrati in formato digitale"³⁰ e SPID come "sistema che consente agli utenti di avvalersi di gestori dell'identità digitale e di gestori di attributi qualificati, per consentire ai fornitori di servizi l'immediata verifica della propria identità e di eventuali attributi qualificati che li riguardano".

La normativa vigente, quindi, impone alle pubbliche amministrazioni di rendere accessibili tramite SPID i servizi in rete erogati che richiedono identificazione informatica (cfr. art. 64, comma 2-*quater*, CAD). Al contempo, però, la stessa normativa riconosce ai privati, ai fini dell'erogazione dei propri servizi in rete, la facoltà di avvalersi del sistema SPID per la gestione dell'identità digitale dei propri utenti (art. 64, comma 2-*quinqüies*, CAD).

La normativa regolamentare sullo SPID in materia di adesione al sistema da parte dei fornitori di servizi online, pertanto, prevede una disciplina differenziata a seconda che il soggetto fornitore aderente sia o meno un ente tenuto a garantire i diritti digitali degli utenti sanciti nella "Carta della cittadinanza digitale".

I fornitori di servizi, dunque, secondo quanto previsto nel Decreto, sono deputati a inoltrare, nell'ambito di un servizio online, le richieste di identificazione informatica dell'utente ai gestori dell'identità digitale e a riceverne l'esito.

Per quanto riguarda ulteriori profili di regolazione tecnica, il d.P.C.M. in esame attribuisce all'Agenzia per l'Italia Digitale il compito di definire con proprio regolamento, tra l'altro, le regole tecniche e le modalità attuative per la realizzazione dello SPID e le modalità di accreditamento dei soggetti aderenti (cfr. art. 4, commi 2 e 3, d.P.C.M.).

Rileva dunque il "*Regolamento recante le modalità attuative dello SPID*" (cfr. Det. D.G. AgID n. 44 del 28 luglio 2015 e ss.mm.ii), che definisce le regole per il rilascio dell'identità digitale all'utente da parte del gestore (*identity provider*), nonché le

modalità di gestione e utilizzo dell'identità digitale. In particolare, con riferimento all'utilizzo dell'identità digitale, rileva l'art. 25 del Regolamento, che disciplina l'autenticazione tramite SPID, ossia «il processo in cui l'utente, usando le proprie credenziali SPID, dimostra la propria identità al gestore dell'identità digitale al fine di accedere a servizi disponibili in rete».

Secondo quanto stabilito nel regolamento, «Le relazioni tra i soggetti coinvolti nel processo (l'utente, il gestore dell'identità digitale, il fornitore di servizi ed, eventualmente, il gestore di attributi qualificati) si evidenziano nelle interazioni necessarie al completamento delle attività che, a partire da una richiesta avanzata dal soggetto titolare di una identità digitale, portano all'autorizzazione o al diniego della fruizione di un servizio erogato da un fornitore di servizi». Tali interazioni determinano la produzione di particolari certificazioni, dette "asserzioni SPID" da parte dell'*identity provider*, che consente l'utilizzo delle stesse da parte dei fornitori di servizi. L'asserzione SPID viene rilasciata una volta che il gestore dell'identità digitale abbia verificato l'identità del soggetto sulla base di credenziali fornite dallo stesso. Se tale verifica ha esito positivo, l'asserzione SPID viene emessa, ad uso del fornitore dei servizi.

L'art. 24 del Decreto "Semplificazioni", intervenendo sull'articolo 64 del CAD, ha disposto l'equiparazione di SPID e CIE e indicato il 28 febbraio 2021 quale data per lo switch off delle modalità diverse di identificazione per l'accesso ai servizi online delle pubbliche amministrazioni da parte dei cittadini (nuovo art. 64, comma 3-*bis*, CAD).

Pertanto, i soggetti di cui all'art. 2, comma 2, lett. a) CAD (solo le pubbliche amministrazioni in senso stretto), a partire da quella data, devono utilizzare esclusivamente i suddetti strumenti di identificazione digitale per l'accesso dei soli cittadini (non si parla anche di imprese e professionisti) ai propri servizi online.

A partire da tale data, è fatto divieto alle pubbliche amministrazioni di rilasciare o rinnovare credenziali per l'identificazione e l'accesso dei

gli strumenti telematici messi a disposizione dalle pubbliche amministrazioni e il punto di accesso di cui all'articolo 64-*bis*, anche attraverso dispositivi mobili» [...].

30. Il d.P.C.M. 24 ottobre 2014 reca "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese" e costituisce normativa di attuazione dell'articolo 64 CAD.

cittadini ai propri servizi in rete diverse da SPID, CIE o CNS, fermo restando l'utilizzo di quelle già rilasciate fino alla loro naturale scadenza e, comunque, non oltre il 30 settembre 2021³¹.

Parallelamente a questi sviluppi nazionali, si sta lavorando anche a livello europeo per creare una identità digitale unica europea. Il Regolamento n. 910 del 2014, noto come "Regolamento eIDAS", aveva già posto le basi per la creazione di un quadro normativo comune per l'identità digitale, le firme elettroniche e altri servizi fiduciari.

Da ultimo, è stato raggiunto un accordo sul Regolamento c.d. "eIDAS 2", che mira a creare il Portafoglio Europeo di Identità Digitale (*European Digital Identity Wallet* – EDIW). Questo permetterà ai cittadini europei di utilizzare una sola identità digitale per accedere ai servizi pubblici e privati in tutta l'Unione europea³².

In attuazione di quanto previsto a livello sovranazionale, si sta lavorando al *wallet* italiano, c.d. "IT Wallet". Il Sistema *IT-Wallet* è istituito dall'art. 20, comma 1, lett. e), d. 2 marzo 2024, n. 19, (convertito, con modificazioni, dalla l. 29 aprile 2024, n. 56), che ha novellato il CAD introducendo l'art. 64-*quater*, recante "Sistema di portafoglio digitale italiano – Sistema IT-Wallet".

L'istituzione del Sistema *IT-Wallet*, per espressa previsione normativa, persegue una duplice finalità: innanzitutto, valorizzare e rafforzare l'interoperabilità tra le banche dati pubbliche attraverso la Piattaforma Digitale Nazionale Dati ("PDND"), di cui all'articolo 50-*ter* del CAD, e, inoltre, favorire la diffusione e l'utilizzo di servizi in rete erogati da soggetti pubblici e privati (cfr. comma 1).

Ai sensi del comma 2, il Sistema *IT-Wallet* si compone di due soluzioni di portafoglio digitale, pubblico e privato. L'*IT-Wallet* pubblico è reso disponibile mediante il punto di accesso telematico di cui all'articolo 64-*bis* del CAD ("app IO")³³.

3. SPID per i minori: le Linee guida dell'Agenzia per l'Italia digitale

Nel contesto normativo appena descritto, il 3 marzo 2022, con Determinazione n. 51, l'Agenzia per l'Italia Digitale ha pubblicato le *Linee guida operative per la fruizione dei servizi SPID da parte dei minori*³⁴. Tali Linee guida intendono definire le modalità di rilascio dell'identità digitale al minore e le modalità di fruizione dei servizi online mediante tale identità.

Anche in questo caso, la *ratio* dell'intervento è la particolare condizione di fragilità riconosciuta al minore. Si legge, infatti, nelle Linee guida che «la normativa vigente consente la creazione dell'identità digitale in favore di tutti i cittadini. Risulta evidente, tuttavia, la necessità di una tutela specifica per un soggetto fragile come il minore».

In particolare, il documento individua le modalità operative che i gestori dell'identità digitale e i fornitori di servizi SPID devono porre in essere al fine di consentire ai minori la fruizione dei servizi in rete in piena sicurezza.

Gli obiettivi, per espressa previsione delle Linee guida, sono: «1. consentire ai minori di acquisire la propria identità digitale, previa richiesta da parte di chi esercita la responsabilità genitoriale; 2. consentire al minore di fruire autonomamente di servizi online mediante la propria identità digitale, ferma restando – salvo casi specifici – la possibilità di autorizzazione e verifica da parte dell'esercente la responsabilità genitoriale; 3. consentire ai fornitori di servizi in rete la selezione dei propri utenti in base all'età».

Più che i profili tecnici, rilevano, in questa sede, i principi fondamentali sottesi al documento.

In primo luogo, emerge il *principio di responsabilità genitoriale*. Le Linee guida attribuiscono un ruolo centrale al genitore, in qualità di esercente la responsabilità genitoriale, nel processo di rilascio

31. Per un approfondimento cfr. BELISARIO-RICCIULLI-PAGNOTTA 2020.

32. Per un approfondimento cfr. MANCA 2024.

33. Per un approfondimento cfr. RICCIULLI 2024.

34. Cfr. il testo della Determinazione. Ai sensi dell'art. 14-*bis* CAD, comma 2, lett. a), infatti, tra le funzioni dell'Agenzia c'è quella di a) emanazione di Linee guida contenenti regole, standard e guide tecniche, nonché di indirizzo, vigilanza e controllo sull'attuazione e sul rispetto delle norme di cui al presente Codice, anche attraverso l'adozione di atti amministrativi generali, in materia di agenda digitale, digitalizzazione della pubblica amministrazione, sicurezza informatica, interoperabilità e cooperazione applicativa tra sistemi informatici pubblici e quelli dell'Unione europea.

e gestione dell'identità digitale SPID del minore. Solo il genitore in possesso di un'identità SPID può richiederne una per il figlio, garantendo un primo livello di controllo e sicurezza. Inoltre, il genitore è costantemente coinvolto attraverso un sistema di notifiche che lo informa delle richieste di accesso del minore ai servizi online, consentendogli di autorizzare o negare l'accesso in base alle proprie valutazioni.

Un secondo principio cardine è quello della *protezione dei dati personali del minore*, declinato secondo i principi del GDPR. Le Linee guida sottolineano, infatti, l'importanza di applicare i principi di liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, aggiornamento, limitazione della conservazione, integrità e riservatezza. In particolare, la procedura di identificazione del minore è stata progettata per richiedere solo i dati strettamente necessari, riducendo al minimo l'esposizione del minore a rischi di privacy.

Le Linee guida promuovono inoltre il principio di *gradualità nell'autonomia del minore*. Si riconosce che il grado di autonomia del minore nell'utilizzo di SPID deve essere commisurato alla sua età e maturità. Per i minori infraquattordicenni, l'accesso è limitato ai servizi essenziali, come quelli scolastici o di prevenzione e consulenza, senza la necessità di autorizzazione genitoriale. Ai minori ultraquattordicenni è concesso un maggiore livello di autonomia, con la possibilità di accedere a un più ampio ventaglio di servizi, previa autorizzazione del genitore. Al compimento della maggiore età, il neo maggiorenne acquisisce il pieno controllo della propria identità digitale, con la possibilità di revocare o mantenere l'identità precedentemente rilasciata. Si ritiene che tale principio risulti fondamentale per la creazione di un'autonoma identità del minore, laddove la scelta di approcci più repressivi potrebbe proteggere ma anche disincentivare lo sviluppo della personalità.

Infine, le Linee guida pongono l'accento sul principio di *flessibilità e adattabilità*. Il sistema di gestione di SPID per i minori è stato progettato per

adattarsi alle diverse esigenze e situazioni, offrendo un elevato grado di personalizzazione. Ad esempio, i gestori dell'identità digitale (IdP) hanno la possibilità di implementare diverse modalità di identificazione del minore, anche in assenza di un numero di telefono cellulare o di un dispositivo mobile. Questa flessibilità garantisce l'inclusione di tutti i minori, a prescindere dalla loro condizione sociale o tecnologica.

Ebbene, posto il generale favore con cui all'epoca fu salutato il provvedimento dell'Agenzia, che si fonda sui condivisibili principi appena esposti, ritengo debbano essere svolte almeno due ordini di riflessioni.

La prima è che SPID per i minori fa parte di una più complessa strategia della governance legata alla volontà di diffondere l'identità digitale e lo strumento SPID. Al netto dell'utilità dello strumento per i fini di verifica dell'età, infatti, la scelta di estendere SPID ai minori ha indubbiamente anche contribuito ad ampliare la platea delle persone che potevano (e in alcuni casi dovevano) dotarsi di un'identità digitale in un momento, come quello che stava vivendo il Paese nel 2022, in cui il Legislatore, a valle della pandemia da Covid-19 e degli investimenti del PNRR, puntava a diffondere l'identità digitale presso fasce sempre più ampie della popolazione.

Si aggiunge che tale strumento, nonostante gli investimenti effettuati anche ad opera del PNRR, presenta ancora diversi limiti. Sebbene, come esposto, lo SPID potrebbe, ai sensi dell'art. 2, comma 3, del CAD, essere reso obbligatorio anche per i servizi resi dai privati oltre che per i soggetti pubblici, gli stessi sarebbero sempre liberi di investire su strumenti di identificazione alternativi. Come esposto, del resto, solo per le pubbliche amministrazioni in senso stretto, ha validità lo "switch off" degli strumenti alternativi previsto dal Legislatore con il "Decreto Semplificazioni". È proprio, però, con riferimento ai servizi privati, soprattutto i social network, che si avverte da anni l'esigenza di regolarne l'accesso. Si registrano, in questo senso, innumerevoli proposte di legge sul tema³⁵.

35. Quelle di Sportiello [C. 1771](#), Bonelli [C.1800](#) e Madia [C.1863](#) sono solo alcune delle proposte di legge sul tema attualmente in discussione.

4. Le più recenti novità della normativa in materia di *age verification* in Europa

Come noto, da anni la normativa in materia di *data protection* ha stabilito regole dedicate e più stringenti agli utenti minorenni³⁶.

Da ultimo, i temi dei servizi digitali e dei diritti degli utenti rispetto agli stessi sono stati profondamente impattati dall'entrata in vigore del Regolamento 2022/2065, Digital services act (c.d. "DSA").

Quest'ultimo, all'articolo 28, prescrive che tutti i fornitori di piattaforme online adottino misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori, anzitutto mediante l'attivazione dei meccanismi di verifica dell'età. Inoltre, ai sensi dell'articolo 35, paragrafo 1, lettera j) del DSA, i fornitori di piattaforme online di dimensioni "molto grandi" e di motori di ricerca online di dimensioni "molto grandi" devono adottare misure di attenuazione dei rischi sistemici, tra cui "misure mirate per tutelare i diritti dei minori, compresi strumenti di verifica dell'età e di controllo parentale, o strumenti volti ad aiutare i minori a segnalare abusi o ottenere sostegno, a seconda dei casi".

Disposizioni analoghe sono contenute nella Direttiva (UE) 2018/1808, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato, recepita in Italia con d.lgs. 208/2021, Testo Unico dei servizi di media audiovisivi (cd. "TUSMA")³⁷.

La normativa sovranazionale, dunque, richiama l'esigenza di meccanismi di *age assurance*³⁸,

stabilendo che i minori hanno diritto ad un livello più elevato di protezione dai contenuti che potrebbero nuocere al loro sviluppo fisico, mentale o morale, anche introducendo misure più rigorose nei confronti di ogni servizio della società dell'informazione.

Alla luce della normativa sovranazionale ma anche in ragione di vicende contingenti, è intervenuto il già citato d.l. 15 settembre 2023, n. 123, convertito con mod. dalla l. n. 159 del 2023, c.d. "Decreto Caivano", recante "Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori in ambito digitale"³⁹.

In particolare, prevede, al Capo IV, "Disposizioni per la sicurezza dei minori in ambito digitale" e, tra le altre cose, nell'ambito dell'art. 13-*bis*, introduce disposizioni per la verifica della maggiore età con specifico riferimento all'accesso a siti pornografici, sulla base della presunzione secondo la quale i contenuti a carattere pornografico minerebbero il rispetto della "dignità" dei minori e ne "compromettono" il "benessere fisico e mentale", comportando, di conseguenza, un problema di "salute pubblica". La disposizione prevede, di conseguenza, al comma 2, che i gestori di siti web e i fornitori delle piattaforme di condivisione video (ovunque stabiliti), che diffondono in Italia immagini e video a carattere pornografico, sono tenuti a verificare la maggiore età degli utenti, al fine di evitare l'accesso a contenuti pornografici da parte di minori degli anni diciotto.

Il Governo ha colto l'occasione anche per ottemperare a quanto previsto dall'art. 49, comma 2, del DSA sui servizi digitali, designando l'Autorità per le garanzie nelle comunicazioni quale Coordinatore dei servizi digitali per l'Italia.

36. Cfr. art. 8 e considerando 38 GDPR, nonché il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101).

37. OROFINO 2022.

38. Con il termine "Age assurance" o "Garanzia dell'età" si intende l'insieme dei metodi, sistemi e processi utilizzati per determinare l'età o la fascia di età di un individuo a vari livelli di confidenza o certezza.

39. Il decreto prende il nome dai gravi fatti avvenuti nel Comune di Caivano, che hanno coinvolto alcuni minori. In particolare, il Governo ha adottato il decreto «Ritenuta la straordinaria necessità e urgenza di introdurre disposizioni per il contrasto alla criminalità minorile e all'elusione scolastica, e per la tutela delle minori vittime di reato» e «la straordinaria necessità ed urgenza di rafforzare la tutela dei minori nello spazio cibernetico e rispetto all'offerta di contenuti e servizi on line, al fine di garantirne il benessere e il pieno sviluppo fisico e mentale».

Ebbene, si ritiene che tale intervento del Governo debba essere letto alla luce dell'approccio scelto anche in altri Paesi europei⁴⁰.

In Francia, ad esempio, la Corte d'appello di Parigi ha emesso una recentissima ordinanza⁴¹ nei confronti di alcuni gestori di siti extraeuropei che offrono contenuti pornografici, in ragione del fatto che tali piattaforme non adotterebbero misure sufficienti per verificare l'età degli utenti. In particolare, in base all'ordinanza, i fornitori di servizi di telecomunicazione sono obbligati a impedire l'accesso a tali siti entro 15 giorni dalla notifica dell'ordine, finché detti siti non avranno adottato un sistema di verifica dell'età più rigoroso. Si legge nell'ordinanza che la Corte ha ritenuto che "l'interesse del minore" sia un "aspetto primario" che giustifica l'eventuale violazione di "altri diritti come la libertà di espressione o di comunicazione".

La Francia, del resto, aveva già adottato una legge che prevede l'obbligo per i siti per adulti di verificare che i minori non accedano ai loro contenuti⁴². Quest'ultima, analogamente al "Decreto Caivano", prevede altresì l'adozione da parte dell'Autorità di regolamentazione della comunicazione audiovisiva e digitale francese (Arcom) di un documento che determini i requisiti tecnici minimi applicabili ai sistemi di verifica, dell'età che devono essere utilizzati dai siti che diffondono contenuti pornografici.

L'Arcom, in data 9 ottobre 2024, ha pubblicato una bozza sottoposta a consultazione pubblica e alla Commissione nazionale per l'informatica e le libertà civili (CNIL)⁴³, che agisce nel Paese quale autorità per la protezione dei dati personali.

In effetti, anche la Commissione europea sta monitorando attentamente la questione della verifica dell'età, che, come anticipato, è considerata una priorità nel contesto del Digital Services Act. In questo senso, a giugno scorso, ha richiesto chiarimenti a piattaforme che offrono contenuti pornografici sulle misure adottate per mitigare i rischi legati alla protezione dei minori online, come previsto dal DSA⁴⁴. Inoltre, il 31 luglio 2024 la Commissione ha pubblicato un invito agli *stakeholder* a presentare contributi volti a sostenere la Commissione per l'elaborazione di orientamenti nel quadro del DSA, al fine di raccogliervi i contributi sull'ambito di applicazione, l'approccio e il contenuto degli orientamenti. Infine, il 14 ottobre 2024 la Commissione ha pubblicato il bando di procedura ad evidenza pubblica per attività di sviluppo, consultazione e supporto per una soluzione di *age verification*⁴⁵. Parallelamente, sotto un altro profilo attinente più strettamente alla questione della protezione dei dati personali, nella seduta del 14 marzo 2024 del Comitato europeo per la protezione dei dati, le autorità nazionali per la protezione dei dati hanno discusso l'attribuzione di un mandato al Comitato stesso ai fini dell'individuazione di criteri per i trattamenti di verifica dell'età, con l'obiettivo di giungere a un approccio coerente e armonizzato per quanto riguarda i principi generali di protezione dei dati da garantire in tale contesto e i requisiti tecnici per detti sistemi, proprio in virtù della sussistenza di diversi obblighi giuridici a introdurre un meccanismo di verifica da parte della normativa unionale (come, per l'appunto, il DSA e l'AVMS).

40. Cfr. sul tema NATALE 2024.

41. *Decisione de la chambre 1-3 de la cour d'appel de Paris sur le blocage de plusieurs sites internet permettant l'accès des mineurs, sur le territoire français, a des contenus pornographiques*, 17 ottobre 2024.

42. Legge n. 2024-449. La legge per la sicurezza e la regolamentazione dello spazio digitale (la "Legge SREN") è stata adottata il 21 maggio e pubblicata nel "Journal Officiel" il 22 maggio. Alcuni dei gestori dei siti hanno avviato azioni legali per contestare l'applicazione della norma.

43. *Référentiel technique sur la vérification de l'âge pour la protection des mineurs contre la pornographie en ligne* del 9 ottobre 2024.

44. Le richieste sono state fatte dopo che queste piattaforme erano state classificate come "grandi piattaforme digitali" ai sensi del DSA lo scorso dicembre. I siti coinvolti hanno successivamente presentato ricorso e le cause sono attualmente tuttora in corso.

45. European Commission, *Call for tenders EC-CNECT/LUX/2024/OP/0073 – Development, Consultancy and Support for an Age Verification Solution*.

5. I principi affermati da AGCOM sui metodi di *age assurance*

L'Autorità per le garanzie nelle comunicazioni è attiva da diversi anni sul tema della tutela dei minori nello spazio digitale⁴⁶.

Da ultimo, con delibera n. 61/24/CONS, in attuazione della l. 13 novembre 2023, n. 159, che dispone la conversione, con emendamenti, del citato “Decreto Caivano”, ha avviato una consultazione pubblica⁴⁷ sugli strumenti di *age assurance*⁴⁸.

A tale consultazione hanno partecipato altre istituzioni, associazioni di categoria e di

consumatori, piattaforme di condivisione video. È stato altresì acquisito parere favorevole del Garante per la protezione dei dati personali⁴⁹ (con qualche precisazione, anche riguardo al metodo più sicuro da utilizzare per la validazione dell'identità dell'utente).

In data 7 ottobre 2024, l'AGCOM ha reso noto che, nella seduta del 24 settembre 2024, a valle della consultazione, è stato approvato uno schema di regolamento⁵⁰ che disciplinerà le modalità tecniche e di processo per l'accertamento della maggiore età degli utenti. Tale schema, in quanto contenente

46. V. delibera n. 9/23/CONS, del 25 gennaio 2023, recante “Adozione delle linee guida finalizzate all'attuazione dell'articolo 7-bis del decreto-legge 30 aprile 2020, n. 28 in materia di sistemi di protezione dei minori dai rischi del cyberspazio”.

47. Cfr. art. 13-bis, commi 3, 4 e 5, d.l. 123 del 2023, i quali recitano: «3. L'Autorità per le garanzie nelle comunicazioni stabilisce, entro sessanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, con proprio provvedimento, sentito il Garante per la protezione dei dati personali, le modalità tecniche e di processo che i soggetti di cui al comma 2 sono tenuti ad adottare per l'accertamento della maggiore età degli utenti, assicurando un livello di sicurezza adeguato al rischio e il rispetto della minimizzazione dei dati personali raccolti in ragione dello scopo. 4. Entro sei mesi dalla data di pubblicazione del provvedimento di cui al comma 3, i soggetti di cui al comma 2 si dotano di efficaci sistemi di verifica della maggiore età conformi alle prescrizioni impartite nel predetto provvedimento. 5. L'Autorità per le garanzie nelle comunicazioni vigila sulla corretta applicazione del presente articolo e, in caso di inadempimento, contesta ai soggetti di cui al comma 2, anche d'ufficio, la violazione, applicando le disposizioni di cui all'articolo 1, comma 31, del decreto legislativo 31 luglio 1997, n. 249, e li diffida ad adeguarsi entro venti giorni. In caso di inottemperanza alla diffida, l'Autorità per le garanzie nelle comunicazioni adotta ogni provvedimento utile per il blocco del sito o della piattaforma fino al ripristino, da parte dei soggetti di cui al comma 2, di condizioni di fornitura conformi ai contenuti della diffida dell'Autorità. Poteri specifici, del resto, sono assegnati all'Autorità dal Testo Unico sui Servizi Media Audiovisivi (TUSMA) a tutela dei minori, articoli 41 e 42, rispetto a contenuti che possano nuocere al loro sviluppo fisico, mentale o morale».

48. Come si legge nelle definizioni dello schema di Regolamento per «“Garanzia dell'età” o “Age assurance” si intende l'insieme dei metodi, sistemi e processi utilizzati per determinare l'età o la fascia di età di un individuo a vari livelli di confidenza o certezza. Le tre categorie principali di metodi di assicurazione dell'età sono l'autodichiarazione, la verifica dell'età e la stima dell'età. Autodichiarazione (di seguito anche Self-declaration) si riferisce all'insieme di processi in cui un utente inserisce una data o seleziona una casella di un form, anche online, per dichiarare di essere sopra/sotto una determinata età, senza fornire altre prove; Stima dell'età (di seguito anche Age estimation) si riferisce ai metodi che stabiliscono che con una certa probabilità un utente abbia una certa età, rientri in una fascia di età o sia superiore o inferiore a una certa età. I metodi di stima dell'età includono l'analisi automatizzata di dati comportamentali e ambientali, confrontando il modo in cui un utente interagisce con un dispositivo o con altri utenti della stessa età, metriche derivate dall'analisi dei movimenti del corpo, il riconoscimento facciale, o l'analisi delle capacità o conoscenze. Nei metodi utilizzati per una stima dell'età rientrano anche quelli effettuati mediante algoritmi e il ricorso a tecnologie basate sull'intelligenza artificiale. Verifica dell'età (di seguito anche Age verification) fa riferimento a quei sistemi che si basano su identificatori rigidi (fisici) e/o fonti di identificazione verificate, che forniscono un elevato grado di certezza nel determinare l'età di un utente».

49. Come previsto dall'art. 13-bis, comma 3, d.l. 123 del 2023.

50. V. *Modalità tecniche e di processo per l'accertamento della maggiore età degli utenti ai sensi dell'articolo 13 bis del decreto legge 5 settembre 2023, n. 123 convertito con modificazioni dalla legge 13 novembre 2023, n. 159*.

disposizioni rientranti nella definizione di “regola tecnica” di cui alla Direttiva (UE) 2015/1535, è stato notificato alla Commissione europea per l'ultimo vaglio. Conseguentemente, in virtù della procedura attivata, l'AGCOM non potrà adottare il regolamento prima del 17 gennaio 2025, salvo eventuali ulteriori estensioni del termine richiesti dalla Commissione ai fini della valutazione di conformità con il diritto unionale.

L'Autorità ha scelto, al fine di non impattare eccessivamente sugli operatori di mercato e di prevenire l'obsolescenza tecnologica, un approccio tecnologicamente neutrale, che consente ai soggetti tenuti alla realizzazione dei processi di *age*

assurance «una ragionevole libertà di valutazione e scelta», stabilendo tuttavia i principi e requisiti che devono essere soddisfatti dai sistemi messi in campo⁵¹.

Rispetto ai contenuti di siti e piattaforme, l'Autorità ha precisato che le modalità tecniche prescelte nell'ambito del provvedimento in oggetto sono “altamente raccomandate” anche con riferimento ad ulteriori tipologie di contenuti, oltre a quelli a carattere pornografico, che potrebbero comunque nuocere allo sviluppo fisico, mentale o morale dei minori quali ad esempio le categorie previste dalla delibera 9/23/CONS⁵².

51. Tali principi sono: *Proporzionalità*: occorre trovare un equilibrio adeguato tra i mezzi impiegati per verificare l'età e l'impatto che tali mezzi possono avere sulla limitazione dei diritti delle persone. *Protezione dei dati personali (riservatezza)*: i sistemi di verifica dell'età devono rispettare le normative sulla protezione dei dati previste dal Regolamento GDPR (UE) 2016/679, garantendo la minimizzazione dei dati, la precisione e la limitazione della conservazione. Non è ammesso il trattamento di dati personali come quelli presenti sui documenti di identità, immagini fotografiche o video, dati delle carte di credito, o altre informazioni personali sensibili. *Sicurezza*: Il sistema di verifica dell'età deve prevedere adeguate misure di sicurezza informatica per ridurre i rischi di attacchi e proteggere il sistema da tentativi di elusione, conformemente al GDPR e alla proposta di Cyber Resilience Act (CRA). *Precisione ed efficacia*: Il sistema deve essere accurato nel determinare l'età, minimizzando gli errori. La verifica dell'età deve essere eseguita ad ogni accesso ai siti o piattaforme di condivisione video che diffondono contenuti pornografici. La validità della verifica termina quando l'utente esce dal servizio, dal browser o quando si verificano eventi come la sospensione del sistema operativo o 45 minuti di inattività. *Funzionalità, accessibilità e facilità d'uso*: I sistemi di verifica dell'età devono essere semplici da utilizzare, adattandosi alle capacità e necessità specifiche dei minori, senza ostacolare l'accesso ai contenuti su Internet. *Inclusività e non discriminazione*: Il sistema di verifica dell'età deve essere progettato in modo da evitare, o almeno minimizzare, qualsiasi forma di pregiudizio o discriminazione involontaria nei confronti degli utenti. *Trasparenza*: Gli operatori devono essere chiari e trasparenti con gli utenti riguardo ai sistemi di verifica dell'età utilizzati, ai dati trattati e alle finalità di tale trattamento. Le spiegazioni devono essere semplici, comprensibili e accessibili sia agli adulti che ai minori. *Formazione e informazione*: È fondamentale educare e sensibilizzare i minori, i genitori e il personale scolastico e giovanile sulle pratiche di sicurezza informatica e sui rischi legati all'uso di Internet. *Gestione dei reclami*: I fornitori dei servizi di verifica dell'età devono garantire un canale dedicato alla gestione rapida dei reclami in caso di errori nel processo di determinazione dell'età.

52. Cfr. schema di Regolamento AGCOM in cui si legge: «Ritenuto opportuno chiarire, viste le osservazioni di alcuni soggetti intervenuti nella consultazione pubblica, che la disciplina delle modalità tecniche e di processo per l'accertamento della maggiore età degli utenti, che con la presente delibera si approva in attuazione dell'art. 13-bis del decreto-legge n. 123/2023 convertito, con modificazioni, dalla legge n. 159/2023, deve essere adottata dai gestori di siti web e dai fornitori delle piattaforme di condivisione video, che diffondono in Italia immagini e video a carattere pornografico ovunque stabilite; Ritenuto, ad ogni buon fine che, alla luce del contesto normativo di riferimento prima richiamato e alle risultanze della consultazione medesima, le modalità tecniche e di processo per l'accertamento della maggiore età degli utenti che con la presente delibera si approvano in attuazione del citato decreto-legge (come convertito in legge) siano altamente raccomandate, in quanto efficaci, idonee, proporzionali e funzionali, per il loro stesso utilizzo anche da parte di altri soggetti rispetto a quelli qui direttamente regolati e con riferimento ad ulteriori tipologie di contenuti, oltre a quelli a carattere pornografico, che potrebbero comunque nuocere allo sviluppo fisico, mentale o morale dei minori quali ad esempio le categorie previste dalla delibera 9/03/CONS».

Fermo restando l'approccio per principi e requisiti generali che lasci gli operatori liberi di scegliere, al fine di garantire il requisito della riservatezza "rafforzata", le specifiche dell'Autorità prevedono un sistema di verifica dell'età che utilizzi il modello del "doppio anonimato", in cui non si deve permettere ai fornitori di verifica dell'età di conoscere il servizio per il quale viene eseguita la verifica, di sapere se due verifiche provengono dalla stessa fonte o se un utente ha già utilizzato il sistema di verifica. Tale modello è quello scelto anche dalla Francia e che si rinviene tra le citate specifiche tecniche approvate dall'ARCOM.

In funzione del requisito appena ricordato, il sistema proposto dall'Autorità prevede l'intervento, per la fornitura della prova della maggiore età, di soggetti terzi indipendenti certificati, attraverso un processo di verifica dell'età che prevede due passaggi logicamente separati: identificazione e autenticazione della persona identificata, per ciascuna sessione di utilizzo del servizio regolamentato (cioè, la fornitura di contenuti pornografici tramite sito o piattaforma web)⁵³.

Ciò ha portato all'esclusione espressa di SPID, che, almeno nella sua conformazione attuale, non garantisce il doppio anonimato.

Nonostante, infatti, l'AGCOM all'interno del documento valorizzi il fatto che, come si è esposto,

i gestori dell'identità digitale sono soggetti terzi essi stessi (sia nei riguardi del soggetto regolamentato, sia rispetto a "enti statali" e gestori di "banche dati pubbliche") e in possesso di determinati requisiti soggettivi e oggettivi stabiliti dalla normativa di settore, selezionati sulla base di specifiche procedure di qualificazione e sottoposti a vigilanza da parte dell'Agenzia per l'Italia Digitale, si legge che «il sistema SPID, ad esempio, non risulta, ai fini dell'attuazione delle disposizioni di cui all'art.13-bis della legge 13 novembre 2023, n. 123, pienamente conforme alle specifiche tecniche AGCOM di seguito indicate (essenzialmente nella parte in cui è prescritto il c.d. doppio anonimato), nel momento in cui si trasferisce all'Identity Provider la richiesta di autenticazione del Service Provider, che contiene il nome a dominio del sito visitato. Infatti, tale sistema di autenticazione SPID consente all'Identity Provider di conoscere il particolare sito/piattaforma visitato dall'utente e non è da escludere che tale informazione venga memorizzata all'interno dei sistemi dell'Identity Provider»⁵⁴.

Di particolare interesse, ai fini del presente contributo, è anche il passaggio dello schema di regolamento sui portafogli digitali. Infatti, si fa espresso riferimento all'identità digitale europea, ricordando che le piattaforme online di dimensioni molto grandi, come definite dal DSA (*Digital Services*

53. Il sistema è diverso a seconda che si parli di sistemi di verifica dell'età non basati su applicativi installati nel terminale utente o di sistemi basati sull'uso di applicativi installati sul dispositivo. Nel primo caso, il processo di verifica dell'età deve essere diviso in tre fasi distinte: 1. Emissione della prova dell'età: La prima fase consiste nell'ottenere una "prova dell'età" attraverso un processo di identificazione gestito da enti indipendenti dal fornitore di contenuti. Questo processo può avvenire, ad esempio, tramite l'accesso a un sito web utilizzando un browser. Gli enti che rilasciano questa prova possono essere fornitori specializzati nella gestione dell'identità digitale o organizzazioni che hanno già verificato l'identità dell'utente in altri contesti. Questi soggetti, che emettono la prova dell'età, non sono a conoscenza del fine per cui l'utente intende utilizzarla. Inoltre, devono essere certificati da un'Autorità competente, che garantisce l'affidabilità del sistema di identificazione adottato. 2. Consegna della prova all'utente: Nella seconda fase, la prova dell'età viene comunicata unicamente all'utente, che avrà la responsabilità di presentarla al sito o alla piattaforma che intende visitare. L'utente può ottenere la prova scaricandola direttamente dal sito dell'ente certificatore e successivamente inviarla autonomamente, attraverso il web, alla piattaforma che richiede la verifica dell'età. 3. Verifica della prova da parte della piattaforma: Infine, la piattaforma o il sito visitato dall'utente esamina la prova dell'età ricevuta e determina se concedere o meno l'accesso al contenuto richiesto. Questa fase rappresenta l'autenticazione dell'età dell'utente, che viene eseguita sulla base della prova fornita. Nel caso, invece, di sistemi di *age assurance* basati sull'uso di applicativi installati sul dispositivo, il soggetto terzo dovrà mettere a disposizione dell'utente una APP per la certificazione e la generazione della "prova dell'età", al fine di consentire all'utente di effettuare l'autenticazione e fornire la prova dell'età al sito web o piattaforma visitata, direttamente utilizzando l'APP installata sul proprio dispositivo e il servizio presente nella piattaforma/sito web deputato a tale scopo.

54. Cfr. all. B al regolamento sezione I.8 "Osservazioni sull'uso di sistemi pubblici".

Act), che impongono agli utenti di autenticarsi per accedere ai servizi online, dovranno accettare anche l'uso dei portafogli europei di identità digitale, anche per quanto riguarda gli attributi minimi necessari per lo specifico servizio online per il quale è richiesta l'autenticazione, come la prova dell'età.

6. Prime conclusioni

In conclusione, si può affermare che SPID nasce come sistema per l'accesso sicuro ai servizi amministrativi e pubblici, nell'ambito dei quali l'identificazione dell'utente è un requisito essenziale. Proprio perché concepito per identificare in modo certo e univoco i cittadini, tale strumento non è in grado di soddisfare le esigenze di anonimato richieste in altri contesti, come l'accesso a contenuti online in cui l'età deve essere verificata senza necessariamente rivelare l'identità dell'utente.

In questo senso, l'identità digitale diventa terreno per riflessioni più ampie relative al bilanciamento di diversi interessi.

Nel contesto descritto, il minore, che gode già di una protezione specifica per via del suo *status*, assume anche i ruoli di "utente", "interessato" e "consumatore" rispetto ai servizi digitali, nonché di "utilizzatore", se questi ultimi sono anche basati su sistemi di intelligenza artificiale. Questa nuova realtà introduce ulteriori rischi e nuove necessità giuridiche in relazione alla tutela dell'identità digitale dei minori.

A livello nazionale e sovranazionale, si assiste, in effetti, a un aumento delle autorità responsabili della protezione dei dati personali, dell'identità digitale e della tutela dei minori nel contesto virtuale. La creazione di nuove figure regolatorie e il moltiplicarsi delle normative possono sembrare, in apparenza, un segnale positivo, anche alla luce della collaborazione interistituzionale che si è manifestata nella realizzazione di tavoli tecnici, protocolli d'intesa e linee guida congiunte.

Tuttavia, sebbene virtuoso, l'interessamento di più autorità potrebbe risultare inefficace nel garantire una protezione coerente e unitaria: l'eccessiva frammentazione rischia, infatti, di generare confusione sia tra i destinatari delle norme (minori, famiglie e imprese), sia tra le stesse istituzioni coinvolte.

Un esempio di questa complessità riguarda l'obbligo di trasparenza di cui, come si è visto, parla

anche il summenzionato schema di regolamento imposto agli operatori per i meccanismi di verifica dell'età, aggiungendosi a quello previsto dalle normative in materia di protezione dei consumatori e degli interessati per ciò che riguarda il trattamento dei loro dati personali. Imporre obblighi di trasparenza, come dimostrato in passato dalla normativa in materia di *data protection*, non garantisce di per sé una maggiore consapevolezza da parte degli utenti: nonostante lo sforzo del GDPR per rafforzare la trasparenza, spesso, le informative privacy, pur essendo dettagliate e obbligatorie, risultano di difficile comprensione, soprattutto per i minori e le loro famiglie. Questa complessità porta frequentemente gli utenti ad accettare termini e condizioni e *privacy policy* senza una piena consapevolezza rispetto alle conseguenze delle proprie scelte.

La trasparenza, dunque, rimane un principio cardine ma con la consapevolezza che da sola non è sufficiente a garantire una comprensione più profonda. Occorre promuovere iniziative di formazione e sensibilizzazione per sviluppare una cultura digitale solida e radicata. In questo senso, è essenziale un intervento non solo normativo, ma anche educativo e culturale, mirato a una formazione capillare rivolta a minori, famiglie e istituzioni scolastiche. L'alfabetizzazione digitale è infatti un fattore cruciale per promuovere una cultura della consapevolezza e della responsabilità nel mondo digitale. Scuole, genitori e tutori devono essere preparati a guidare i minori verso un utilizzo consapevole delle tecnologie e delle piattaforme online. La crescita equilibrata dell'identità digitale richiede un approccio integrato, probabilmente più complesso di quello attualmente adottato a livello nazionale.

A tale proposito, l'approccio repressivo e settoriale scelto dal Governo italiano rischia di non affrontare efficacemente i pericoli reali per i minori. Il Legislatore, o il Governo in sua vece, dovrebbe evitare interventi mossi dalla contingenza (come nel caso del d.l. "Caivano") e settoriali e adottare piuttosto una visione globale e integrata dei rischi digitali, ponendo attenzione particolare a tutti i fenomeni e gli ambiti (si pensi al gioco d'azzardo), che rappresentano effettivamente una minaccia per i minori. Anche dal confronto con l'approccio francese emerge che, sebbene in entrambe le esperienze ci si concentri a livello normativo esclusivamente sui contenuti pornografici, la scelta francese

si fonda sull'analisi di dati⁵⁵ ed è assunta tramite uno atto normativo ordinario e non eccezionale come è (o almeno dovrebbe essere), invece, la decretazione d'urgenza in Italia.

Non è un caso che l'AGCOM abbia altamente raccomandato le modalità tecniche prescelte nell'ambito del provvedimento adottato dalla stessa anche con riferimento ad ulteriori tipologie di contenuti, oltre a quelli a carattere pornografico, che potrebbero comunque nuocere allo sviluppo fisico, mentale o morale dei minori.

Non si tratta solo di un tema di opportunità ma anche di legittimità. Solo nei prossimi mesi sarà possibile testare la tenuta del sistema delle fonti approntato dall'ordinamento italiano sul tema. Del resto, l'art. 13-*bis* del citato "Decreto Caivano" forse

costituiva regola tecnica e non è stato notificato alla Commissione europea, con la conseguenza che la stessa delega ad AGCOM per adottare il regolamento sarebbe inficiata. Qualche dubbio sorge anche con riferimento alla compatibilità del 13-*bis* con il principio del "*country-of-origin*", pilastro della Direttiva e-Commerce.

Sarà fondamentale dunque valutare come si evolveranno le reazioni istituzionali e giudiziarie. Da un lato, i giudici nazionali potrebbero essere chiamati a pronunciarsi sulla conformità della norma alle disposizioni europee, dall'altro, la Commissione europea potrebbe aprire una procedura di infrazione qualora ritenesse che il "Decreto Caivano" violi i principi e le regole del mercato unico digitale.

Riferimenti bibliografici

- G. ALPA (2021), *Il diritto di essere se stessi*, La nave di Teseo, 2021
- M. ARE (1965), *Interesse alla qualificazione e tutela della personalità*, in "Rivista del diritto commerciale", 1965, n. 1
- T. ASCARELLI (1957), *Teoria della concorrenza e dei beni immateriali*, Giuffrè, 1957
- C. BASSU (2021), *Il diritto all'identità anagrafica. Il cognome materno tra personalità individuale e principio di eguaglianza*, Editoriale Scientifica, 2021
- E. BATTELLI (a cura di) (2021), *Diritto privato delle persone minori di età. Diritti, tutele, nuove vulnerabilità*, Giappichelli, 2021
- E. BELISARIO, F. RICCIULLI, S. PAGNOTTA (2020), *Amministrazione digitale, guida ragionata agli switch off*, Maggioli, 2020
- A. DE CUPIS (1949), *Il diritto all'identità personale*, Giuffrè, 1949
- D. DI SABATO (2011), *Il contratto del minore tra incapacità di contrarre e capacità di consumare*, in "Rivista di diritto dell'impresa", 2011, n. 1
- G. FINOCCHIARO (2010), (voce) *Identità personale (diritto alla)*, in "Digesto Discipline Privatistiche - Sezione Civile", V agg., Utet Giuridica, 2010
- L.M. FRIEDMAN (2002), *La società orizzontale*, il Mulino, 2002
- P. GLEASON (1983), *Identifying Identity. A Semantic History*, in "The Journal of American History", vol. 69, 1983, n. 4
- K. HETERINGTON (1998), *Expression of identity. Space, Performance, Politics*, SAGE Publications, 1998
- A. IANNUZZI, F. LAVIOLA (2023), *I diritti fondamentali nella transizione digitale fra libertà e uguaglianza*, in "Diritto costituzionale", 2023, n. 1

55. Nel citato provvedimento dell'ARCOM si fa riferimento a ricerche che dimostrano che «2,3 milioni di minori visitano siti pornografici ogni mese» e che «la percentuale di minori che visitano siti "per adulti" è aumentata di 9 punti in 5 anni, passando dal 19% alla fine del 2017 al 28% alla fine del 2022».

- M. LUCIANI (2018), *Quale identità?*, in A. Somma, A. Fusaro, G. Conte, V. Zeno-Zencovich (a cura di), "Dialoghi con Guido Alpa", Roma Tre-Press, 2018
- G. MANCA (a cura di) (2024), *Il regolamento eIDAS n. 2024/1183*, in "Rivista elettronica di Diritto, Economia, Management", n. spec., 2024, n. 4
- A. MORELLI (2019), *Persona e identità personale*, in "BioLaw Journal – Rivista di BioDiritto", 2019, n. 2
- V. NATALE (2024), *Tutela dei minori online: possibili soluzioni per un'accurata verifica dell'età*, in "Agenda Digitale.eu", 6 giugno 2024
- M. OROFINO (2022), *La normativa a tutela dei minori nel Testo Unico per la fornitura di servizi di media audiovisivi con uno sguardo rivolto al regolamento (UE) 2022/2065*, in "MediaLaws", 2022, n. 3
- G. PINO (2010), *Identità personale*, in S. Castignone, L. Lombardi Vallauri (a cura di), "Trattato di biodiritto", Giuffrè, 2010
- G. PINO (2003), *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, il Mulino, 2003
- E.C. RAFFIOTTA (2010), *Appunti in materia di diritto all'identità personale*, in "Forum di Quaderni Costituzionali", 26 gennaio 2010
- A. RANDAZZO (2021), *Diritto all'identità personale e valori costituzionali. Le linee di un modello, traendo spunto da Luigi Pirandello*, in "dirittifondamentali.it", 2021, n. 3
- G. RESTA (2007), *Identità personale e identità digitale*, in "Il Diritto dell'informazione e dell'informatica", 2007, n. 3
- M. RICCA (2008), *Oltre Babele: codici per una democrazia interculturale*, edizioni Dedalo, 2008
- F. RICCIULLI (2024), *I diritti digitali: verso un'identità unica europea*, in "Diritto Pubblico Europeo – Rassegna Online", 2024, n. 1
- P. STANZIONE (2014), *I contratti del minore*, in "Europa e diritto privato", 2014, n. 4
- P. STANZIONE, G. SCIANCALEPORE (2006), *Minori e diritti fondamentali*, Giuffrè, 2006
- L. TRUCCO (2004), *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, Giappichelli, 2004



GIOVANNI BAROZZI REGGIANI

Protezione dei minori dai contenuti nocivi circolanti sulle *Video Sharing Platforms*: un'ipotesi di (ir)ragionevolezza legislativa?

Il contributo si interroga sulle esigenze di protezione dei minori rispetto ai contenuti nocivi circolanti sulle *Video Sharing Platforms* (VSP), muovendo da un inquadramento costituzionale di tali esigenze e procedendo con una riflessione sul necessario bilanciamento tra le stesse e altri diritti e beni costituzionali (e in particolare la libertà di iniziativa economica e di manifestazione del pensiero) che vengono in rilievo rispetto a discipline volte a limitare la circolazione dei contenuti medesimi. Inquadrate in via generale il tema, il contributo si sofferma su alcune disposizioni del vigente Testo unico dei servizi media audiovisivi che attribuiscono ad AGCOM poteri specifici nei confronti dei fornitori di servizi di VSP, esprimendo una valutazione sulla ragionevolezza di tali disposizioni anche in riferimento alle esigenze di “fondamento scientifico” che paiono emergere in riferimento a detti poteri.

Piattaforme di condivisione di video – Protezione dei minori – Contenuti nocivi – AGCOM – Norme science-based

The protection of minors from harmful content provided on video sharing platform services. An inquiry into the solutions provided by the Italian legal framework

The paper aims to investigate the legal framework (both European and Italian) concerning the protection of the minors from harmful content provided on video-sharing platform services. The paper examines how the stated objective – protecting minors from harmful content – can be accomplished in the digital ecosystem. Establishing a legal framework for the protection of minors, particularly one that allows a public Authority to restrict the dissemination of harmful content, as provided by the Italian legal system, implies limiting some constitutional freedoms of both service providers and users of those services. This suggests, in accordance to the Italian Constitution, that the public Authority's prerogatives must be grounded in science, rather than just being reasonable and proportionate. Regarding this last topic, the paper analyzes how the Italian legal system ensures that “scientific basis”.

Video sharing platforms – Protection of minors – Harmful contents – AGCOM – Evidence-based legislation

L'Autore è ricercatore di Istituzioni di diritto pubblico presso l'Università di Sassari

Questo contributo fa parte della sezione monografica *Minori e Internet* a cura di Carlo Colapietro e Antonio Iannuzzi

SOMMARIO: 1. L'intrinseca pericolosità della Rete e la necessità di una regolazione "di protezione" per i minori. – 2. Lo sviluppo e il benessere psico-fisico dei minori quale bene costituzionalmente protetto e il quadro giuridico in materia di *Video Sharing Platforms*. – 3. La ragionevolezza delle vigenti disposizioni per la protezione dei minori dalla circolazione di contenuti su servizi VSP e il tema del fondamento scientifico dei poteri di AGCOM.

1. L'intrinseca pericolosità della Rete e la necessità di una regolazione "di protezione" per i minori

La navigazione in Internet è attività che espone chi la compie a potenziali pericoli, alcuni dei quali concernono direttamente l'esercizio di diritti e libertà costituzionalmente tutelati.

Ciò è dovuto, almeno in parte, alle caratteristiche intrinseche della Rete.

Quest'ultima configura infatti un luogo – cui è relativamente semplice accedere da parte di una platea molto vasta di utenti – nel quale è possibile reperire una quantità virtualmente infinita di informazioni e svolgere molte delle attività della nostra quotidianità¹.

La Rete è dunque certamente spazio di diritti (e libertà); al contempo, all'interno della stessa risulta molto difficile controllare, quantomeno con tempestività ed efficacia, le attività che vengono svolte dagli utenti, in ragione della rapidità con cui vengono scambiati dati e informazioni e delle caratteristiche dei servizi che costituiscono il veicolo di tali scambi (c.d. "*Over The Top* – OTT"²), la gran parte dei quali svolge funzioni di hosting e di diffusione dei contenuti caricati dagli utenti (attività, quest'ultima, caratterizzante in particolare le piattaforme online³).

L'accesso a tali servizi è del resto molto agevole, essendo usualmente condizionato alla sola accettazione delle regole definite dal singolo fornitore nell'ambito delle condizioni generali di utilizzo (di

1. Sulla pervasività della penetrazione della "tecnologia" nella nostra vita quotidiana v., tra gli altri, COLAPIETRO 2021, p. 8.

2. «Si considerano rientranti nel concetto di Over the Top quelle imprese che forniscono, attraverso la rete Internet, servizi, contenuti e applicazioni di tipo "rich media". Esse traggono ricavo, in prevalenza, dalla vendita di contenuti e servizi agli utenti finali o di spazi pubblicitari e si rivolgono ad un mercato globale con spese di gestione ed organici ridottissimi» (GATTI 2019, p. 718).

3. L'art. 3, par. 1, lett. i) del Regolamento [2022/2065/UE](#) (*Digital Services Act*) definisce «piattaforma online» un servizio «di memorizzazione di informazioni che, su richiesta di un destinatario del servizio, memorizza e diffonde informazioni al pubblico, tranne qualora tale attività sia una funzione minore e puramente accessoria di un altro servizio o funzionalità minore del servizio principale e, per ragioni oggettive e tecniche, non possa essere utilizzata senza tale altro servizio e a condizione che l'integrazione di tale funzione o funzionalità nell'altro servizio non sia un mezzo per eludere l'applicabilità del presente regolamento». La rilevanza dei servizi OTT per lo svolgimento di attività di vita quotidiana, e i "luoghi di confronto" che i medesimi (ed in specie le piattaforme online) sono in grado di creare, hanno spinto la dottrina a rilevare come tali spazi privati siano entrati «prepotentemente a far parte della sfera pubblica» (BASSINI 2019, p. 15; POLLICINO-DE GREGORIO 2021, p. 6) e a interrogarsi sulla loro qualificabilità in termini di "public fora", cui sarebbe necessario riconoscere la natura di servizio pubblico, o comunque di attività a rilevanza pubblicistica (BASSINI 2022, p. 311 ss.).

natura contrattuale) che – rispetto ai più rilevanti fra i servizi *OTT*, e in specie le piattaforme online – prevedono sovente limitazioni riferite tanto allo *status* e alle condizioni personali o giuridiche degli utenti⁴, quanto ai contenuti che possono essere veicolati tramite lo specifico servizio.

Peraltro, la violazione delle condizioni generali di utilizzo può determinare conseguenze di vario tipo (impossibilità per l'utente di continuare a utilizzare il servizio, il sorgere di profili di responsabilità civile o penale, e così via), ma di per sé non impedisce la circolazione di dati e contenuti (determinandone al più la successiva sospensione o cessazione) che dal momento della loro diffusione possono in brevissimo tempo giungere a conoscenza di un pubblico più o meno vasto⁵ e produrre effetti lesivi di situazioni giuridiche soggettive di singoli individui (o enti) o di beni o valori che un ordinamento giuridico considera per sé rilevanti⁶.

A ciò aggiungasi che le condizioni di utilizzo dei servizi non hanno storicamente impedito la creazione di profili falsi o il proliferare di *bot* e *trolls*.

Appare chiaro, alla luce di tutto ciò, come sulla Rete sia difficile controllare non solo chi accede, ma anche come opera.

Del resto, il fatto che molti dei menzionati effetti negativi discendono da attività che configurano espressione di diritti e libertà cui gli ordinamenti accordano una particolare protezione – e

specificamente la libertà di manifestare il pensiero, cardine dell'ordinamento democratico⁷, e quella di svolgere attività economica – ha reso storicamente complicata la messa a punto di discipline atte a contrastare alcuni dei fenomeni più perniciosi, quali *fake news*, disinformazione e discorsi d'odio (che traggono alimento dalla «bulimia informativa (e pseudoinformativa) offerta dal web e dalle Internet Platforms [che] mette in crisi la capacità di discernere il vero dal falso, conferendo la stessa forma al reale e alla finzione»⁸) o a contrastare la diffusione di contenuti suscettibili di ledere la sensibilità di alcuni soggetti.

Le principali difficoltà sono connesse a diversi fattori, legati, da un lato, alla esatta individuazione del bene o del valore costituzionale che occorre, di volta in volta, salvaguardare, dall'altro alle specifiche libertà che verrebbero incise dalle relative discipline legislative «di protezione».

Riguardo al profilo da ultimo citato, si osserva che la condivisione di contenuti tramite piattaforme online è attività che riguarda indubbiamente la manifestazione del pensiero degli utenti e l'iniziativa economica dei fornitori dei servizi; in riferimento a questi ultimi, peraltro, potrebbe venire in rilievo a sua volta la libertà di manifestazione del pensiero, specie se si abbandonasse quell'approccio – dedotto anche in specifiche disposizioni normative, ma che il progresso della tecnologia (e

4. A titolo di esempio, le condizioni contrattuali di Facebook prevedono che ai servizi della piattaforma non possano accedere utenti infra-tredicenni o soggetti condannati per violenza sessuale o il cui account sia stato precedentemente disabilitato per violazione delle medesime condizioni, degli standard della community o di normative e condizioni che si applicano all'utilizzo della piattaforma, o ancora «gli utenti non autorizzati dalla legge applicabile a ricevere» prodotti, servizi o software erogati dall'operatore economico (Meta).

5. Alla base del concetto di piattaforma vi è proprio l'idea del servizio che consente «l'interazione (fisica o virtuale) fra due (o più) gruppi interdipendenti di utenti» (PERRUCCI-FRANCOLA-MENSAH 2023, p. 47).

6. Sui limiti che derivano alla definizione delle condizioni di utilizzo del servizio dalla necessità di rispettare i quadri giuridico-normativi degli ordinamenti v. le interessanti riflessioni di RUFFOLO 2023, cap. VI, par. 2.

7. Della libertà di manifestazione del pensiero come della «pietra angolare dell'ordine democratico» parlò espressamente la Consulta nella sentenza n. 84 del 1969 (in termini assimilabili si pronunciarono le precedenti sentenze nn. 9 e 25 del 1965), mentre nella successiva pronuncia n. 126 del 1985 la Corte si esprime, a riguardo della libertà in parola, come di «cardine di democrazia nell'ordinamento generale». Allo stesso filone devono poi essere ricondotte le sentenze n. 11 del 1968, che definì il diritto di cui all'art. 21 Cost. «coessenziale al regime di libertà garantito dalla Costituzione», e n. 98 del 1968, secondo cui la «libertà di manifestazione del pensiero [...] è ordine dell'ordinamento democratico». Sulla garanzia della libertà di manifestare il pensiero quale elemento caratterizzante lo Stato democratico (e a questo in qualche modo «consustanziale») v., in dottrina, tra gli altri, PACE-MANETTI 2006, p. 37 ss.; LUCIANI 1989, p. 606; PALADIN 1987, p. 6; ESPOSITO 1958, p. 12.

8. IANNUZZI 2024, p. 12. Su questi temi v. anche COLAPIETRO 2022, p. 422 ss.

il progressivo raffinarsi dei processi di elaborazione dei dati su base algoritmica) rende giorno dopo giorno più discutibile – che esclude la sussistenza, in capo ai fornitori di servizi di piattaforme online, e specie quelle di condivisione di video (di seguito anche solo VSP), di forme di responsabilità editoriale⁹.

Infine, si pone il tema della proporzionalità delle misure, e la loro conciliabilità con la natura e le modalità di funzionamento dei servizi, i fornitori dei quali sono peraltro soggetti ad uno speciale regime di responsabilità¹⁰.

La necessità di dirimere tali complessi nodi ha portato, sino ad oggi, a tentativi di regolazione di taluni aspetti dei servizi *OTT* – effettuati in

particolare nell'ambito dell'ordinamento europeo – tutto sommato timidi e, quantomeno fino all'entrata in vigore del citato *Digital Services Act*¹¹ e della Direttiva 2018/1808/UE (cosiddetta SMAV2, che ha introdotto la prima disciplina specificamente dedicata alle VSP, modificando a tal fine la Direttiva 2010/13/UE), affidati in larga misura a strumenti quali la co-regolamentazione e l'auto-regolamentazione¹², cui peraltro l'ordinamento europeo dimostra di non voler affatto rinunciare¹³.

Per le descritte ragioni, se pare esservi una concordia di base e trasversale (in quanto condivisa da istituzioni e dottrina) sulla necessità di regolare taluni fenomeni, tra cui la circolazione di contenuti “disturbanti” per talune categorie, quando

9. Ai sensi dell'art. 1, par 1, lett. c) della Direttiva [2010/13/CE](#), come modificata dalla Direttiva 2018/1808/UE, la responsabilità editoriale si configura laddove sia rinvenibile «l'esercizio di un controllo effettivo sia sulla selezione dei programmi sia sulla loro organizzazione in un palinsesto cronologico, nel caso delle radiodiffusioni televisive, o in un catalogo, nel caso dei servizi di media audiovisivi a richiesta». La sussistenza di una simile forma di responsabilità è espressamente esclusa, per le VSP, dalla stessa definizione di «servizio di piattaforma per la condivisione di video» (di cui all'art. 1, lett. a *bis*, della Direttiva). Tale impostazione appare invero criticabile nella misura in cui, come è stato osservato, è ormai evidente come le piattaforme online non svolgano più «un ruolo meramente neutrale rispetto al contenuto veicolato in Rete, anche solo per l'organizzazione dello stesso» (ALBANESI 2024, pp. 76 e 78).

10. Trattasi del regime definito, nell'ambito dell'ordinamento europeo, dalla c.d. Direttiva e-commerce ([2000/31/CE](#)) la quale, tra le altre cose, prevede, in riferimento ai fornitori di servizi di *mere conduit*, caching e hosting, il principio dell'assenza di un obbligo generale di sorveglianza sui contenuti caricati dagli utenti (all'art. 15) e quello secondo cui un *hosting provider* non possa essere considerato responsabile per le informazioni memorizzate su richiesta di un destinatario del servizio a condizione che «a) non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione, o b) non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso» (art. 14). Tale regime di responsabilità – rispetto al quale la giurisprudenza amministrativa e della Corte di Giustizia ha elaborato la distinzione fra hosting providers attivi e hosting providers passivi – è stato confermato dal *Digital Services Act* (cfr. in particolare artt. da 4 a 8). Su questi temi, per tutti, v. il recente contributo di VACCARI 2024.

11. Cfr. nt. 2.

12. Sui richiamati istituti si rimanda al *Parere del Comitato economico e sociale europeo sul tema «Autoregolamentazione e coregolamentazione nel quadro legislativo dell'UE»* ([2015/C 291/05](#)), che ben delinea le differenze tra gli stessi. In dottrina, per tutti, si rimanda a SIMONCINI 2022.

13. Per quanto di interesse, l'art. 4-*bis* della Direttiva 2010/13/UE, introdotto dalla Direttiva 2018/1808/UE (di cui ampiamente si dirà), dispone che «gli Stati membri incoraggiano il ricorso alla coregolamentazione e la promozione dell'autoregolamentazione tramite codici di condotta adottati a livello nazionale nei settori coordinati dalla presente direttiva nella misura consentita dai loro ordinamenti giuridici [...]». Invero, pare emergere una preferenza per la co-regolamentazione, in quanto considerata più efficace della autoregolamentazione, come sottolineato dall'*European Parliamentary Research Service* in uno studio pubblicato nel febbraio 2021 dal titolo «Liability of online platforms». Per considerazioni sull'idoneità e sull'efficacia di quella particolare forma di co-regolamentazione rappresentata dall'adozione di Codici di condotta si rimanda alle interessanti osservazioni di POLLICINO 2022.

si passa al piano della concreta messa a punto di discipline legislative o regolamentari emergono molti distinguo e incertezze; e ciò mantenendosi in ambito continentale: uno sguardo a quanto accade (ed è accaduto) Oltreoceano – che per ragioni di brevità il presente contributo non può che limitarsi a richiamare – mostra infatti come la stessa necessità di regolare tali fenomeni costituisca un dato tutt'altro che acquisito, risultando ancora tanti (e determinati) i difensori della metafora del *free marketplace of ideas*, per sua natura refrattaria a forme di regolazione della libertà di manifestazione del pensiero¹⁴.

Ciò premesso, si osserva che l'affermazione secondo cui navigare in Internet configura attività intrinsecamente pericolosa risulta particolarmente vera rispetto ai minori, esposti a rischi specifici e rilevanti (per numero e qualità).

Detta “particolare esposizione” si deve, prevalentemente, al minor livello di consapevolezza dei minori (rispetto agli adulti) circa il modo in cui “funziona” la Rete, vengono erogati i servizi *OTT* e possono venir esercitati, tramite essi, diritti e libertà¹⁵.

Tale constatazione evoca esigenze di protezione, che tuttavia non sussistono solo in riferimento a ciò che accade sulla Rete, avendo piuttosto portata generale: i minori sono non a caso fatti oggetto di discipline giuridiche il cui scopo è proprio quello di salvaguardarne diritti e interessi, tramite istituti che non di rado prevedono il prodursi di determinati effetti giuridici a prescindere da volontà contrarie espresse dai minori stessi ovvero da parte di loro eventuali tutori e/o rappresentati legali.

A discipline di tal fatta sono indubbiamente riconducibili gli obblighi normativi di contrasto alla circolazione di contenuti nocivi per i minori da parte dei fornitori di VSP, che costituiscono l'oggetto principale delle riflessioni del presente lavoro.

Ciò premesso, nell'ottica di effettuare qualche considerazione (anche di sistema) sul tema, si procederà, seguendo l'ordine ricostruttivo in

precedenza delineato, a inquadrare, da un punto di vista costituzionale, il bene giuridico protetto.

2. Lo sviluppo e il benessere psico-fisico dei minori quale bene costituzionalmente protetto e il quadro giuridico in materia di Video Sharing Platforms

A livello tanto europeo quanto di ordinamento interno si rinvencono diverse disposizioni il cui scopo specifico è quello di preservare i minori dall'esposizione a contenuti che possano ledere lo sviluppo fisico, mentale o morale.

Nella Carta costituzionale, invero, non vi sono disposizioni volte espressamente a tutelare tale bene giuridico, né specularmente un obbligo per chiunque diffonda contenuti suscettibili di ledere il medesimo di adottare misure e cautele atte a scongiurare tale rischio.

Tuttavia, la copertura costituzionale per discipline legislative riferite a detti profili non può essere revocata in dubbio.

Tale copertura può infatti, in primo luogo, ricondursi a esigenze di tutela della salute umana, quale diritto (fondamentale) del singolo e interesse della collettività (e dunque all'art. 32 Cost.).

Ai sensi, poi, dell'art. 41, comma secondo, Cost., l'iniziativa economica privata «non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla salute, all'ambiente, alla sicurezza, alla libertà, alla dignità umana», mentre l'art. 31 stabilisce, tra le altre cose, che fra i compiti dell'insieme dei pubblici poteri – riconducibili al concetto di Repubblica – vi sia quello di proteggere «la maternità, l'infanzia e la gioventù, favorendo gli istituti necessari a tale scopo».

È sufficiente, ritengo, il richiamo a tali disposizioni per affermare l'astratta conformità alla Carta di discipline limitative tanto della iniziativa economica privata quanto della manifestazione del pensiero (in ragione della sussistenza dei limiti impliciti alla stessa individuati

14. Sulla metafora del *free marketplace of ideas* – espressione che fu utilizzata espressamente nella sentenza della Corte Suprema statunitense *United States v. Rumely* del 1953, da parte del Justice Douglas, ma la cui originaria formulazione si deve alla nota *dissenting opinion* espressa dal Justice Holmes nel caso *Abrams v. United States* del 1919 – per brevità si rimanda ai contributi di RAMAJOLI 2018 e DE GREGORIO 2017 e ai riferimenti dottrinali ivi citati.

15. Sulla particolare “pericolosità” della Rete per i minori cfr. MUSSELLI 2011, *passim*.

dalla Corte costituzionale¹⁶, che si aggiungono a quello, espressamente contemplato dal comma sesto dell'art. 21, del «buon costume»), salva poi la necessità di verificarne in concreto la ragionevolezza e la proporzionalità.

La copertura giuridica (anche costituzionale) per le esigenze di salvaguardia dello sviluppo e del benessere psico-fisico dei minori è poi ulteriormente rafforzata dall'esistenza di atti e convenzioni internazionali, oltre che di specifiche disposizioni di diritto europeo, che espressamente o implicitamente contemplano tale finalità.

Nello specifico, a livello internazionale la Convenzione sui diritti dell'infanzia, approvata dall'Assemblea Generale delle Nazioni Unite il 20 novembre 1989, e ratificata dall'Italia il 27 maggio 1991 con la legge n. 176, contiene almeno due disposizioni – gli articoli 6 e 17 – concernenti specificamente il tema in esame¹⁷.

Una menzione può poi essere fatta alla Carta dei diritti fondamentali dell'Ue, nella quale, oltre al diritto alla salute (art. 35) è riconosciuto quello dei minori «alla protezione e alle cure necessarie per il loro benessere» (art. 24, par. 1).

Come detto, le disposizioni convenzionali e sovranazionali ora riportate offrono un ulteriore appiglio per l'individuazione di un fondamento costituzionale a discipline volte a porre regole, per i creatori e i diffusori di contenuti, atte a preservare lo sviluppo psico-fisico ed il benessere dei minori; il carattere costituzionale del fondamento è in questo caso dato dall'art. 117, che come noto pone la regola del necessario rispetto degli obblighi

internazionali e unionali da parte della potestà legislativa.

Alla luce di quanto riportato appare difficilmente confutabile l'affermazione secondo la quale la salvaguardia dello sviluppo e del benessere psico-fisico dei minori costituisca un bene giuridico a rilevanza costituzionale, cui corrisponde un diritto dei minori stessi, necessitante di specifica tutela da parte dei pubblici poteri (e *in primis* dal legislatore).

Non a caso, alla protezione dei minori dall'esposizione a contenuti suscettibili di nuocere allo sviluppo e al benessere dei medesimi sono state dedicate diverse discipline legislative, stratificatesi negli anni; per brevità, ci limiteremo qui a richiamare sinteticamente quelle concernenti i servizi media audiovisivi.

Senza risalire troppo indietro nel tempo, si osserva che già la Direttiva 89/552/CEE, meglio nota come Direttiva TV senza frontiere (le cui disposizioni sono state recepite, almeno in parte, dalla legge n. 223 del 1990, c.d. legge Mammi), sottolineava con forza l'importanza della protezione dei minori, stabilendo che gli Stati membri dovessero controllare che i programmi suscettibili di nuocere allo sviluppo dei medesimi, trasmessi in chiaro, fossero preceduti da un idoneo segnale acustico o identificati da un simbolo visibile, mentre il successivo Codice di autoregolamentazione media e minori (approvato all'assemblea plenaria della Commissione per l'assetto del sistema radiotelevisivo il 5 novembre 2002 e sottoscritto dalle emittenti e dalle associazioni firmatarie il 29 novembre 2002) affermava il diritto di ogni

16. I limiti impliciti erigibili – per via legislativa – alla libertà di manifestare il pensiero risultano giustificati dalla necessità di tutelare altri beni e valori espressamente considerati dalla Costituzione (in tema, tra le altre, cfr. le sentenze della Consulta nn. 20 del 1994, 25 del 1965; 87 e 100 del 1966; 199 del 1972; 15, 16 e 133 del 1973).

17. L'art. 6 concerne la garanzia del diritto alla vita dei fanciulli, e impone agli Stati parti (al comma secondo) di assicurare a questi ultimi nella misura massima possibile «la sopravvivenza e lo sviluppo»; l'art. 17 pone invece l'obbligo per gli Stati parti di assicurare che il fanciullo possa «accedere a una informazione e a materiali provenienti da fonti nazionali e internazionali varie, soprattutto se finalizzati a promuovere il suo benessere sociale, spirituale e morale nonché la sua salute fisica e mentale». Tra i sotto-obblighi riconducibili al riportato obbligo generale, rileva in particolare quello di cui al punto 5 della disposizione da ultimo richiamata, concernente l'elaborazione, da parte degli Stati parti, di «principi direttivi appropriati destinati a proteggere il fanciullo dalle informazioni e dai materiali che nuocciono al suo benessere in considerazione delle disposizioni degli artt. 13 e 18» (la prima concernente la libertà di manifestazione del pensiero dei fanciulli, che comprende anche il diritto a ricevere informazioni, la seconda concernente la responsabilità genitoriale in relazione al mantenimento e allo sviluppo del fanciullo). Riferimenti allo sviluppo, al benessere e alla salute fisica e mentale dei minori si rinvencono anche in diverse altre disposizioni della Convenzione, ancorché in riferimento a temi specifici.

minore a «essere tutelato da trasmissioni televisive che possano nuocere alla sua integrità psichica e morale, anche se la sua famiglia è carente sul piano educativo», prevedendo specifici obblighi, per gli aderenti, atti a garantire l'effettività di tale diritto.

Interventi di rilievo sono da ascrivere anche alla legge n. 112 del 2004 (legge Gasparri), che ha introdotto la distinzione tra televisione ad accesso libero e condizionato (art. 4, comma 1, lett. b), codificato il Codice di autoregolamentazione TV e minori (art. 10, comma 1), previsto l'obbligo di adozione di specifiche misure per la tutela dei minori nella fascia 16-19 e prescritto l'adozione di una disciplina volta a regolare la presenza dei minori in video.

Il d.lgs. 31 luglio 2005, n. 177, recante il Testo unico dei servizi di media audiovisivi e radiofonici (TUSMAR), poneva poi la tutela «del benessere, della salute e dell'armonico sviluppo fisico, psichico e morale del minore» (art. 3, comma 1) fra i principi fondamentali del sistema dei servizi di media audiovisivi e della radiofonia, dettando disposizioni recanti obblighi specifici per tutti i fornitori di tali servizi e obblighi ulteriori per il concessionario del servizio pubblico.

La stessa impostazione, ancorché con qualche elemento di differenziazione, si rinviene nel d.lgs. 8 novembre 2021, n. 208, recante il nuovo Testo unico per la fornitura di servizi di media audiovisivi (TUSMA), che dedica alla tutela dei minori ben quattordici articoli, ponendo regole anche per i contenuti diffusi tramite servizi VSP forniti da soggetti sottoposti alla giurisdizione italiana.

Proprio la diffusione di tali contenuti sembra porre esigenze di tutela fino a tempi recenti sconosciute, come affermato anche dalla Direttiva 2018/1808, che parla apertamente di «nuove sfide» poste da tali piattaforme anche in riferimento alla tutela dei minori rispetto alla esposizione a contenuti nocivi (Considerando 45) e dal *Digital Services Act*.

Quest'ultimo, oltre a porre in capo ai fornitori di servizi intermediari principalmente destinati ai minori (o da questi utilizzati) l'obbligo di spiegare in modo comprensibile condizioni e restrizioni del servizio (art. 14), e ai fornitori di piattaforme

online accessibili ai minori – tra i quali possono essere annoverati anche i fornitori di VSP – l'obbligo di adottare «misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori sul loro servizio» (art. 28, par. 1), prevede che le piattaforme online e i motori di ricerca di dimensioni molto grandi – categoria, la prima, che anche in questo caso può ricomprendere le VSP – debbano effettuare una mappatura dei c.d. rischi sistemici «derivanti dalla progettazione o dal funzionamento del loro servizio e dei suoi relativi sistemi, compresi i sistemi algoritmici, o dall'uso dei loro servizi», compresi quelli concernenti la produzione di effetti negativi per i minori e in generale «per il benessere fisico e mentale della persona» (art. 34, par. 1 e spec. lett. d) e definire misure atte ad attenuare tali rischi (art. 35).

Analogamente, la Direttiva 2010/13/UE (come modificata dalla Direttiva 2018/1808/UE) pone in capo agli Stati membri l'obbligo di assicurare che i fornitori di VSP soggetti alla loro giurisdizione adottino misure adeguate per tutelare «i minori da programmi, video generati dagli utenti e comunicazioni commerciali audiovisive che possano nuocere al loro sviluppo fisico, mentale o morale» (art. 28-ter, par. 1). Tali misure devono essere determinate «alla luce della natura del contenuto in questione, del danno che possono causare, delle caratteristiche della categoria di persone da tutelare nonché di tutti i diritti e gli interessi legittimi, compresi quelli dei fornitori della piattaforma per la condivisione di video e degli utenti che hanno creato o caricato contenuti, nonché dell'interesse pubblico generale», e risultare praticabili e proporzionate «tenendo conto delle dimensioni della piattaforma per la condivisione di video e della natura del servizio offerto» (art. 28-ter, par. 2)¹⁸.

Gli Stati membri sono tenuti a garantire (anche attraverso il ricorso alla co-regolamentazione, ai sensi dell'art. 28-ter, par. 4) che i fornitori di VSP attuino le previste misure e ad adottare meccanismi volti a valutare l'adeguatezza delle stesse, mentre agli utenti delle piattaforme deve essere garantito l'accesso a meccanismi di risoluzione extragiudiziale delle controversie insorte con i fornitori e la

18. La Direttiva, inoltre, definisce un elenco di misure adottabili, dai fornitori, tra cui la messa a punto di sistemi di *age verification* degli utenti delle VSP «per quanto attiene ai contenuti che possano nuocere allo sviluppo fisico, mentale o morale dei minori» (art. 28-ter, par. 3, lett. f).

possibilità di far valere i propri diritti dinanzi ad organi giurisdizionali.

Le richiamate disposizioni europee sono state recepite nell'ambito del TUSMA, ed è proprio sulle disposizioni del Testo unico concernenti gli obblighi di contrasto alla circolazione di contenuti nocivi per i minori sui servizi di VSP che si incentreranno le riflessioni del prossimo paragrafo, al fine di valutarne la ragionevolezza e la proporzionalità, e la conseguente conformità al quadro costituzionale.

Si precisa che tali riflessioni riguarderanno le limitazioni alla circolazione dei contenuti derivanti dall'azione di pubblici poteri; restano invece escluse valutazioni attinenti al tema di limitazioni connesse a iniziative degli stessi fornitori dei servizi di VSP, che restano confinante ad un piano "privatistico" (pur avente anche rilievo pubblicistico) e per le quali la Direttiva prevede la necessaria garanzia dell'accesso per gli utenti a procedure di risoluzione extragiudiziale delle controversie e della possibilità per i medesimi di ricorrere all'autorità giudiziaria contro la rimozione dei contenuti o la disattivazione degli account.

3. La ragionevolezza delle vigenti disposizioni per la protezione dei minori dalla circolazione di contenuti su servizi VSP e il tema del fondamento scientifico dei poteri di AGCOM

Rispetto alla protezione dei minori da contenuti nocivi "circolanti" su servizi di VSP, due sono le principali disposizioni del TUSMA che vengono in rilievo: l'art. 42, che pone in capo ai fornitori di tali servizi soggetti alla giurisdizione italiana l'obbligo di adottare misure volte a tutelare «i minori

da programmi, video generati dagli utenti e comunicazioni commerciali audiovisive che possano nuocere al loro sviluppo fisico, mentale o morale» (comma 1, lett. a), prevedendo a tal fine la promozione di «forme di co-regolamentazione e di autoregolamentazione tramite codici di condotta» (comma 3), e l'art. 41, che assegna ad AGCOM il potere di limitare, per le medesime finalità, la circolazione di programmi, comunicazioni commerciali e video generati dagli utenti veicolati da una piattaforma VSP stabilita in altro Stato membro e diretti al pubblico italiano (art. 41, comma 7, lett. a), e di definire con proprio regolamento la procedura per l'adozione dei relativi provvedimenti (art. 41, comma 9)¹⁹.

Così definita in via di estrema sintesi la disciplina di riferimento, la prima considerazione che può avanzarsi attiene al fatto che il legislatore nazionale (in ciò vincolato da quello europeo) ha espressamente scartato l'ipotesi più restrittiva, per le sfere giuridiche di *uploader* e fornitori di servizi, rappresentata dalla previsione di controlli *ex ante* (mediante filtraggio già nella fase di upload²⁰) che è stata espressamente invece prevista rispetto ad altri ambiti (ed in particolare, in sede unionale, dalla Direttiva 2019/790/UE sul diritto d'autore e sui diritti connessi nel mercato unico digitale).

Il legislatore europeo, e a cascata quello nazionale, ritengono dunque accettabile un certo grado di potenziale vulnerabilità degli interessi dei minori in nome della garanzia della proporzionalità degli obblighi tecnico-organizzativi imposti ai fornitori di servizi VSP²¹ e del contrasto ai rischi di censura preventiva della libertà di manifestazione del pensiero degli utenti, che può peraltro assumere la forma di censura privata (se e nella

19. AGCOM ha dato attuazione alla disposizione in parola con delibera [298/23/CONS](#).

20. V. in questo senso in particolare l'art. 28-ter, par. 3, della Direttiva [2018/1808](#), il quale appunto esclude che le misure da adottarsi, da parte dei fornitori di servizi di VSP, possano condurre alla messa a punto di strumenti «di controllo *ex ante* o al filtraggio dei contenuti nel momento in cui vengono caricati che non siano conformi all'articolo 15 della direttiva 2000/31/CE».

21. Centrale appare la valutazione circa la proporzionalità delle misure anche considerato che la Corte di Giustizia (nella sentenza della Grande sezione del 26 aprile 2022, C-401/19, *Polonia c. Parlamento europeo e Consiglio dell'Unione europea*, paragrafi 39 ss.) ha giudicato giustificate le restrizioni alla libertà di manifestazione del pensiero – tutelata dall'articolo 10 della CEDU e dall'articolo 11 della Carta dei diritti fondamentali dell'Unione – derivanti dall'imposizione di obblighi ai fornitori di servizi di condivisione di contenuti online (peraltro quelli particolarmente gravosi previsti dalla Direttiva [2019/790](#)) in ragione della loro strumentalità a tutelare un bene giuridico rilevante, per l'ordinamento europeo, e proprio della loro proporzionalità.

parte in cui il controllo venisse rimesso alle stesse piattaforme²²).

Il divieto di misure di filtraggio operanti *ex ante* (in fase di upload) e la logica dell'intervento *ex post* non possono infatti garantire l'azzeramento dei rischi per i minori, specie rispetto a modalità di diffusione dei contenuti che possono diventare virali, rendendo conseguentemente impossibile individuarne gli esatti percorsi di circolazione.

Una seconda considerazione attiene poi alla scelta legislativa di rimettere ad un'Autorità indipendente (AGCOM) la verifica dell'adeguatezza delle misure (e la definizione di criteri per la redazione dei codici di condotta) e l'adozione di provvedimenti limitativi della circolazione dei contenuti.

Tale previsione non pare sollevare di per sé profili di compatibilità con il quadro costituzionale: effettuato infatti il bilanciamento in astratto (concernente l'affermazione della limitabilità della libertà di iniziativa economica e di manifestazione del pensiero al fine di tutelare diritti e interessi dei minori, in una logica "protettiva") è necessariamente in riferimento alla prassi, e dunque ai singoli contenuti e alla loro modalità di diffusione che si pone il tema della verifica dell'effettiva lesività (reale o potenziale) dei contenuti stessi per lo sviluppo fisico, mentale o morale dei minori o, per quanto concerne i poteri previsti dall'art. 42, dell'adeguatezza delle misure; né pare porsi un problema relativo al fatto che libertà fondamentali di individui e operatori vengono limitate da un provvedimento di un'Autorità facente parte di quel novero di Enti di cui si lamenta la carenza di legittimazione democratica (le Autorità indipendenti) considerato che il tipo di potere che AGCOM è chiamata ad esercitare pare espressione di quella che viene comunemente definita discrezionalità tecnica.

Tale ultima affermazione si spiega in ragione del fatto che ciò l'Autorità è chiamata a fare è verificare se lo specifico contenuto (o categoria di

contenuti) possa risultare nocivo per lo sviluppo e il benessere psicofisico dei minori, attività che pare avere – quantomeno in riferimento all'intervento *ex post*, sprovvisto della "copertura" fornita dalla normativa europea – natura tecnica, con esclusione di qualsiasi ponderazione tra interessi, che resta dunque quella effettuata "a monte" dal legislatore²³.

Ciò detto, appare utile avviare qualche riflessione sul "tipo di tecnica" che viene in rilievo in riferimento al potere di cui è titolare AGCOM.

Ed infatti, la valutazione circa il carattere nocivo (per i minori) di un contenuto, o categoria di contenuti, sembra richiedere, necessariamente, l'acquisizione dei contributi forniti da una o più branche delle scienze (ed in specie quelle che studiano lo sviluppo e il benessere dei minori da un punto di vista medico-psicologico e altre più attente agli aspetti sociologici della condizione del minore): si tratterebbe, in questo senso, di un potere il cui esercizio richiede un "necessario fondamento scientifico", ovvero di potere rispetto al quale il dato scientifico contribuisce «alla determinazione del concreto ambito di applicazione delle norme costituzionali»²⁴, e dunque alla individuazione del bene tutelato e alla definizione delle concrete modalità di tutela dello stesso.

Il tema è se AGCOM possieda tali competenze specialistiche e, in caso di risposta negativa, come possa colmare tale "lacuna" acquisendo i (necessari) contributi della scienza nell'ambito dei propri processi decisionali (che, lo si ricorda, incidono su diritti e libertà fondamentali di individui e operatori) stante il silenzio della disciplina legislativa sul punto.

In questo senso, e nell'ottica di individuare un elemento di comparazione e raffronto, giova osservare che, in riferimento ai servizi audiovisivi e radiofonici, il TUSMA prevede che AGCOM vigili sul rispetto dei divieti (previsti dall'art. 37) di diffusione di trasmissioni televisive e programmi nocivi

22. In tema cfr. ALBANESI 2024, p. 78; GRANDINETTI 2022, spec. p. 180 ss.

23. Peralto, dal punto di vista della salvaguardia di diritti e libertà, appare non inutile rilevare che la discrezionalità tecnica è "pienamente controllabile" dal Giudice amministrativo, ancorché tramite uno scrutinio che consente al giudice di calarsi negli accertamenti e nelle valutazioni, anche grazie agli strumenti processuali di cui dispone, per verificarne correttezza e attendibilità, senza poter tuttavia sostituire la propria valutazione a quella dell'Amministrazione ove non emergano errori tecnici o scelte manifestamente irragionevoli (in questo senso v., *ex multis*, le sentenze del Consiglio di Stato n. 3854 del 2024, n. 8523 del 2023; n. 3075 del 2021; n. 1958 del 2020).

24. È quanto osservato da PENASA 2015, p. 278, in riferimento a temi afferenti la tutela del diritto alla salute, e in generale l'ambito di applicazione dell'art. 32 Cost.

per «lo sviluppo fisico, psichico o morale dei minori», ed eserciti i relativi poteri sanzionatori (di cui all'art. 38) sentendo il Comitato consultivo interistituzionale istituito presso il MIMIT – dal correttivo al TUSMA di cui al d.lgs n. 50 del 2024 – e avente compiti «di promozione e ricerca sui temi di alfabetizzazione mediatica e digitale e di espressione di un parere nella fase di adozione dei codici di autoregolamentazione e co-regolamentazione dei fornitori di servizi media diffusi tramite qualsiasi canale o piattaforma, a tutela dei minori» (così l'art. 8, comma 2, del TUSMA)²⁵.

Nell'esercizio dei predetti compiti in riferimento ai servizi audiovisivi, per espressa previsione legislativa AGCOM deve dunque interfacciarsi con un organo cui possono ascrivere competenze specialistiche in materia di tutela dello sviluppo e del benessere dei minori.

Qualcosa di simile accade anche rispetto ai poteri e alle prerogative di cui AGCOM è titolare ai sensi dell'art. 42 del TUSMA – e in particolare quelle concernenti la citata promozione dei codici di condotta per l'adozione delle misure (anche) a tutela dei minori e la definizione di linee guida indicanti i criteri specifici relativi all'adozione dei codici²⁶ – anche se il citato correttivo di cui al d.lgs n. 50 del 2024 ha «ridimensionato» il numero degli organi o degli Enti con cui AGCOM deve «interfacciarsi»²⁷.

Di converso, rispetto ai poteri di limitazione della circolazione di contenuti su servizi VSP di cui all'art. 41 del TUSMA, non si prevede il coinvolgimento di alcun altro Ente o organo, di talché AGCOM agisce esercitando esclusivamente la propria discrezionalità (tecnica).

La scelta del Legislatore appare significativa, specie se rapportata a quanto fatto in relazione all'art. 38 del TUSMA, ma anche allo stesso art. 42.

Le ragioni di tali differenze nelle discipline potrebbero forse spiegarsi in ragione delle esigenze di celerità che caratterizzano le attività da esplicarsi ai sensi dell'art. 41, comma 7; tuttavia, a tale osservazione «giustificante» può obiettarsi che la relativa procedura prevede tanto un'ipotesi di azione in via di urgenza quanto una «ordinaria», la quale ultima pare del tutto compatibile con momenti di acquisizione di apporti, contributi e valutazioni di provenienza «esterna».

Più in generale, ci si può domandare se il legislatore avrebbe potuto (o dovuto), in ragione di un possibile «vincolo costituzionale», dettare regole atte a proceduralizzare l'acquisizione, da parte di AGCOM, dell'apporto di organismi tecnico-scientifici (pur nella consapevolezza delle richiamate esigenze di celerità che la natura stessa dei servizi impongono, anche nell'ordinarietà) o volte a prevedere una necessaria «interlocuzione» con enti o organi dotati di competenze

25. Occorre rilevare che l'art. 37, probabilmente a causa di un errore materiale, contiene un riferimento al «Comitato di applicazione del Codice di autoregolamentazione media e minori».

26. Nello specifico, nel testo originario l'art. 42 prevedeva, al comma 3, che AGCOM dovesse provvedere a promuovere l'adozione di codici di condotta, al fine dell'adozione delle misure di protezione dei minori, «sentito il Comitato di applicazione del Codice di autoregolamentazione media e minori». Inoltre, il successivo comma 5 stabiliva che AGCOM definisse le linee guida per recante i criteri per la definizione dei codici «sentiti l'Autorità garante per l'infanzia e l'adolescenza e il Comitato di applicazione del Codice di autoregolamentazione media e minori». Nel testo risultante a seguito delle modifiche apportate dal correttivo, non si rinviene più alcun riferimento al Comitato, «sostituito» dal MIMIT per quanto concerne la definizione delle linee guida, mentre la promozione dei codici di condotta è rimessa alla sola Autorità.

27. Nello specifico, nel testo originario l'art. 42 prevedeva al comma 3, che AGCOM dovesse provvedere a promuovere l'adozione di codici di condotta, al fine dell'adozione delle misure di protezione dei minori, «sentito il Comitato di applicazione del Codice di autoregolamentazione media e minori». Inoltre, il successivo comma 5 stabiliva che AGCOM definisse le linee guida per recante i criteri per la definizione dei codici «sentiti l'Autorità garante per l'infanzia e l'adolescenza e il Comitato di applicazione del Codice di autoregolamentazione media e minori». Nel testo risultante a seguito delle modifiche apportate dal correttivo, per quanto concerne la definizione delle linee guida non si rinviene più alcun riferimento al Comitato, «sostituito» dal MIMIT (e non già dal Comitato consultivo interistituzionale di cui all'art. 8, comma 2, ciò che pone il tema della sua «utilizzabilità» da parte del Ministero) mentre la promozione dei codici di condotta è rimessa alla sola Autorità.

specialistiche a riguardo della tutela dello sviluppo e del benessere dei minori.

In tema si osserva che la sussistenza di un rapporto di connessione tra il (necessario) fondamento scientifico di una disciplina legislativa e l'effettività della tutela dello specifico valore/bene che la medesima si prefigge di tutelare è affermazione ormai consolidata nella giurisprudenza costituzionale (si possono richiamare, tra le tante, le sentenze n. 114 del 1998, n. 282 del 2002, n. 307 del 2003 e n. 151 del 2009), che afferma peraltro la sindacabilità, da parte della Corte, della c.d. "attendibilità scientifica" dell'intervento legislativo (sentenza n. 171 del 2023, spec. § 3.3. Cons. Dir.).

Ciò detto, rispetto allo scrutinio di costituzionalità di leggi che – pur effettuando un bilanciamento in astratto – rimettano la limitazione di diritti e libertà di rilievo costituzionale (ai fini della tutela di beni o valori di pari rango) ad un'Autorità amministrativa, il tema centrale, che pare emergere e definirsi con sempre maggior chiarezza, con il passare del tempo, è proprio quello della procedimentalizzazione, nell'ambito dei processi decisionali, dell'acquisizione dei contributi tecnico-scientifici²⁸.

Sul punto possono richiamarsi le due sentenze della Consulta concernenti lo stabilimento dell'Ilva di Taranto, la n. 85 del 2013 e la n. 58 del 2018.

La prima ha dichiarato non fondata la questione (*rectius*: una delle questioni) di costituzionalità sottopostale (declinata in termini di ragionevolezza della specifica disciplina che veniva in rilievo) per il fatto che la definizione del punto di equilibrio fra prosecuzione dell'attività imprenditoriale e tutela dell'ambiente e della salute umana era rimessa ad un atto da adottarsi all'esito di un procedimento – quello dell'A.I.A. e del suo riesame – che prevedeva un ruolo specifico per organismi tecnico-scientifici, il ricorso alle migliori tecniche

disponibili per l'individuazione delle misure atte a prevenire gli impatti ambientali e istituti atti a garantire la partecipazione del pubblico.

A conclusioni opposte è giunta invece la sentenza n. 58 del 2018 (che si è espressamente confrontata con quella del 2013) proprio per l'assenza di un'adeguata procedimentalizzazione delle attività per la definizione delle misure atte a garantire la tutela dell'ambiente e della salute.

Nello stesso solco si colloca poi anche la recente sentenza n. 105 del 2024, la quale, pur rigettando la questione sottopostale, ha posto l'accento sulla necessità che un'attività amministrativa – volta a tutelare beni e/o valori di rango costituzionale limitando specularmente diritti e libertà – che tratti "temi" la cui definizione richiede il necessario apporto delle scienze, sia preceduta da adeguata istruttoria e risulti «sorretta da una congrua motivazione, che dia conto tra l'altro delle risultanze dell'istruttoria» (§ 5.4.1 Cons. Dir.), effettuando quella che aveva tutta l'aria di costituire una "delega di bilanciamento" all'Autorità amministrativa²⁹.

Rispetto al descritto quadro, si osserva nuovamente che nel caso dell'art. 41 del TUSMA – del quale potrebbe peraltro porsi in dubbio la compatibilità con il diritto europeo, e in particolare con le disposizioni della Direttiva *e-commerce* che vietano agli Stati membri di «limitare la libera circolazione dei servizi società dell'informazione provenienti da un altro Stato membro» salvo che per le ragioni indicate dalla Direttiva stessa³⁰ – la deduzione dei contributi dei saperi specialistici nei procedimenti e nei provvedimenti limitativi della circolazione dei contenuti nocivi per i minori tramite servizi di VSP non risulta (adeguatamente) procedimentalizzato.

Ciò detto, il quesito che si pone è se tale scelta legislativa si mostri idonea a configurare un vizio di ragionevolezza della disciplina, in riferimento

28. Sul tema della procedimentalizzazione dell'acquisizione dei contributi scientifici nei procedimenti decisionali (e in particolare legislativi) v., per tutti, IANNUZZI 2018, p. 179 ss.

29. Su tale figura MODUGNO 2007, pp. 34-35; BIN 1992, p. 88 ss.

30. Il par. 4 dell'art. 3 della Direttiva 2000/31/CE stabilisce che gli Stati membri possano adottare provvedimenti in deroga a quanto stabilito per il perseguimento di determinate finalità (tra cui la tutela dell'ordine pubblico, «in particolare per l'opera di prevenzione, investigazione individuazione e perseguimento in materie penali, quali la tutela dei minori e la lotta contro l'incitamento all'odio razziale, sessuale, religioso o etnico, nonché violazioni della dignità umana della persona» e la tutela della sanità pubblica). Tali misure devono risultare necessarie al perseguimento dei richiamati fini, riferirsi a un determinato servizio della società dell'informazione e risultare proporzionate.

alla protezione del bene giuridico “sviluppo e benessere psicofisico del minore” (e dunque alle disposizioni costituzionali e convenzionali sopra richiamate) o quale parametro alla stregua del quale valutare le limitazioni alla libera manifestazione del pensiero o all'attività economiche di utenti delle piattaforme di VSP e fornitori delle medesime.

Sul punto, occorre osservare che un eventuale scrutinio della Corte ben difficilmente si spingerebbe oltre una valutazione di eventuale manifesta irragionevolezza della disciplina (che si potrebbe eventualmente porre solo laddove AGCOM risultasse del tutto “inadeguata” alla funzione, ciò che non pare), e che si rinvergono comunque elementi atti a “contenere” la discrezionalità (tecnica) dell'Autorità, la quale può attingere ad un bagaglio di prassi e di esperienza di contrasto ai contenuti nocivi ampio (formatosi in materia di SMAV, che pure presentano dinamiche diverse dai servizi VSP) e giovare delle interlocuzioni con la Commissione e delle attività dell'ERGA, oltre al fatto che le linee guida da definirsi ai sensi dell'art. 42, se fossero estese anche alla definizione dei contenuti nocivi (e non solo alle misure), ridurrebbero a loro volta i margini di discrezionalità, peraltro sempre sindacabile dal Giudice amministrativo il quale, come si è detto, è in grado di “entrare”, anche eventualmente a mezzo del ricorso ai mezzi istruttori di cui dispone, ai sensi del c.p.a., nelle valutazioni dell'Autorità, verificando correttezza e ragionevolezza, come anche una recente pronuncia resa in termini di SMAV conferma³¹.

A ciò aggiungasi che l'Autorità potrebbe comunque acquisire *sua sponte* contributi tecnici, ovvero auto-vincolarsi in tal senso a mezzo di apposite disposizioni regolamentari³²; tale considerazione, per quanto indubbiamente vera e corretta, non inficia il giudizio di preferibilità di una procedimentalizzazione (riguardo al profilo in parola) effettuata per via legislativa, che avrebbe (avuto) il pregio di vincolare AGCOM ad uno schema di processo decisionale definito dal legislatore (riguardo, eventualmente, all'organismo o agli organismi da consultare, alle modalità per l'acquisizione dei contributi di questi ultimi, alla natura giuridica e agli effetti che i medesimi sono destinati a produrre sul procedimento e sulla decisione finale, e così via), offrendo anche in questo caso al Giudice parametri più certi per esercitare il proprio scrutinio.

Sarà poi interessante verificare l'impatto che su questo tema (ed altri) avrà l'attività dei c.d. segnalatori attendibili, soggetti che, ai sensi dell'art. 22 del DSA, possono presentare alle piattaforme online segnalazioni “qualificate” sulla circolazione di taluni contenuti, tra cui (come indicato da AGCOM nella delibera 283/24/CONS), quelli concernenti «violazioni delle norme a tutela dei minori: condivisione di contenuti che possono nuocere allo sviluppo fisico, psichico e morale dei minori, mancata attuazione di restrizioni specifiche in base all'età per i minori, pedopornografia, adescamento di minori, ecc...» (Allegato 2, lett. h)³³.

31. Il riferimento, nello specifico, va a Cons. Stato, Sez. VI, 10 luglio 2024, n. 6144.

32. Sul punto si osserva che non paiono idonee a soddisfare le esigenze espresse (specie in termine di creazione di un auto-vincolo) le previsioni di cui all'art. 5, commi 2 e 3 del Regolamento AGCOM allegato alla delibera 298/23/CONS. La prima stabilisce che la Direzione, nello svolgimento dell'attività pre-istruttoria funzionale all'avvio di un procedimento ex art. 41 TUSMA, acquisisca «ogni elemento necessario, anche attraverso ispezioni, richieste di informazioni e documenti, audizioni e segnalazioni»; la seconda dispone invece che «ai fini dello svolgimento dell'attività di vigilanza, la Direzione si può avvalere del supporto del Gruppo di Radiodiffusione Editoria incardinato nell'ambito del Nucleo Speciale Beni e Servizi della Guardia di Finanza e della Sezione della Polizia postale e delle comunicazioni della Polizia di Stato secondo i protocolli d'intesa sottoscritti con l'Autorità». Tali disposizioni non sembrano configurare un autovincolo procedimentale all'acquisizione di contenuti tecnico-scientifici “specialistici” riguardo la tutela dei minori dall'esposizione a contenuti nocivi, apparendo riferite più alla fase dell'acquisizione di elementi fattuali-istruttori che non ad una “valutazione” (anche tecnico-scientifica) degli stessi.

33. Trattasi di soggetti che, al fine di ottenere la relativa qualifica, devono dimostrare: a) di disporre di capacità e competenze particolari ai fini dell'individuazione, dell'identificazione e della notifica di contenuti illegali; b) di essere indipendenti da qualsiasi fornitore di piattaforme online; c) di svolgere le proprie attività al fine di presentare le segnalazioni in modo diligente, accurato e obiettivo (art. 22, par. 2, DSA). Tra le competenze previste,

Alla luce di ciò, si ritiene che anche l'attività dei segnalatori attendibili potrà fornire, nel tempo, elementi utili a "guidare" la discrezionalità di AGCOM.

Tutti i descritti profili, se non eliminano il tema della verifica del necessario fondamento scientifico dei procedimenti di competenza di AGCOM, e specie quelli volti ad adottare i provvedimenti previsti dall'art. 41, comma 7, del TUSMA, ne attenuano la portata, o quantomeno lo "rinviano" alla (eventuale) sede giurisdizionale.

Ciò detto, sarebbe stato in ogni caso auspicabile (e lo è tuttora, in una prospettiva *de iure condendo*)

un intervento del legislatore atto a inserire qualche passaggio procedimentale che assicurasse, in termini più certi e "visibili" (proprio in quanto regolati), il fondamento tecnico dello specifico processo decisionale³⁴, nell'ottica di scongiurare conferimenti di troppo ampie deleghe di bilanciamento ad AGCOM o ad organi giurisdizionali, a maggior garanzia delle libertà e dei diritti fondamentali coinvolti nell'attività di *enforcement* dell'Autorità.

Riferimenti bibliografici

- E. ALBANESI (2024), *Le Linee-guida dell'Agcom sugli influencer nella prospettiva dell'attività di informazione e del costituzionalismo digitale*, in "Rivista italiana di informatica e diritto", 2024, n. 1
- M. BASSINI (2022), *Social Networks as New Public Forums? Enforcing the Rule of Law in the Digital Environment*, in "The Italian Review of International and Comparative Law", vol. 1, 2022, n. 2
- M. BASSINI (2019), *Internet e libertà d'espressione. Prospettive costituzionali e sovranazionali*, Aracne, 2019
- R. BIN (1992), *Diritti e argomenti. Il bilanciamento degli interessi nella giurisprudenza costituzionale*, Giuffrè, 1992
- C. COLAPIETRO (2022), *Libera manifestazione del pensiero, fake news e privacy, oggi*, in "Dirittifondamenti.it", 2022, n. 2
- C. COLAPIETRO (2021), *Le sfide del "Costituzionalismo digitale": un approccio originale al rapporto tra diritto e nuove tecnologie*, in "Rivista del Gruppo di Pisa", 2021, n. 3
- G. DE GREGORIO (2017), *The marketplace of ideas nell'era della post-verità: quali responsabilità per gli attori pubblici e privati online?*, in "Media Laws", 2017, n. 1
- C. ESPOSITO (1958), *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Giuffrè, 1958
- A. GATTI (2019), *Istituzioni e anarchia nella rete. I paradigmi tradizionali della sovranità alla prova di internet*, in "Il Diritto dell'informazione e dell'informatica", 2019, n. 3
- O. GRANDINETTI (2022), *Le piattaforme digitali come "poteri privati" e la censura online*, in "Rivista italiana di informatica e diritto", 2022, n. 1
- A. IANNUZZI (2024), *Metaverso, digital twins e diritti fondamentali*, in "Rivista italiana di informatica e diritto", 2024, n. 2
- A. IANNUZZI (2018), *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Editoriale Scientifica, 2018
- A. IANNUZZI (2017), *Istruttoria e valutazioni tecnico-scientifiche*, in "Rivista del Gruppo di Pisa", 2017, n. 1

l'Allegato 1, n. 3, lett. a) della delibera 283/24/CONS annovera peraltro quelle di tipo «tecnico e/o scientifico, definibile come quell'insieme di conoscenze teoriche e pratiche afferenti alla specifica area (o aree) di competenza».

34. Sulla procedimentalizzazione quale tecnica per rendere più "visibile" il fondamento scientifico del processo decisionale v. IANNUZZI 2017, che si riferisce nello specifico ai processi normativi e legislativi (ma con considerazioni che ritengo applicabili anche alla fattispecie qui in commento).

- M. LUCIANI (1989), *La libertà di informazione nella giurisprudenza costituzionale italiana*, in “Politica del diritto”, 1989, n. 4
- F. MODUGNO (2007), *La ragionevolezza nella giustizia costituzionale*, Editoriale Scientifica, 2007
- L. MUSSELLI (2011), *Internet e tutela dei minori*, in “Il Diritto dell’informazione e dell’informatica”, 2011, n. 6
- A. PACE, M. MANETTI (2006), *Art. 21. La libertà di manifestazione del proprio pensiero*, in G. Branca, A. Pizzorusso, “Commentario della Costituzione”, Rapporti civili, Zanichelli, 2006
- L. PALADIN (1987), *Libertà di pensiero e libertà di informazione: le problematiche attuali*, in “Quaderni costituzionali”, 1987, n. 1
- S. PENASA (2015), *Il dato scientifico nella giurisprudenza della Corte costituzionale: la ragionevolezza scientifica come sintesi tra dimensione scientifica e dimensione assiologica*, in “Politica del diritto”, 2015, n. 2
- A. PERRUCCI, V. FRANCOLA, G.A. MENSAH (2023), *Natura e ruolo delle piattaforme digitali, con particolare riferimento ai servizi di pagamento e al credito alla clientela retail*, in C. Giannotti, A. Perrucci (a cura di), “Piattaforme digitali e servizi di pagamento”, Egea, 2023
- O. POLLICINO (2022), *I codici di condotta tra self-regulation e hard law: esiste davvero una terza via per la regolazione digitale? Il caso della strategia europea contro la disinformazione online*, in “Rivista trimestrale di diritto pubblico”, 2022, n. 4
- O. POLLICINO, G. DE GREGORIO (2021), *Constitutional Law in the Algorithmic Society*, in H.-W. Micklitz, O. Pollicino, A. Reichman et al. (eds.), “Constitutional Challenges in the Algorithmic Society”, Cambridge University Press, 2021
- M. RAMAJOLI (2018), *I pericoli del marketplace of ideas. Considerazioni sparse a latere di due sentenze della Corte di giustizia in tema di assegnazione delle frequenze radiotelevisive*, in “Media Laws”, 2018, n. 1
- U. RUFFOLO (2023), *Piattaforme e metaverso*, in C. Pinelli, U. Ruffolo, “I diritti nelle piattaforme”, Giappichelli, 2023
- A. SIMONCINI (2022), *La co-regolazione delle piattaforme digitali*, in “Rivista trimestrale di diritto pubblico”, 2022, n. 4
- S. VACCARI (2024), *Riflessioni sulla responsabilità dei c.d. hosting providers tra enforcement privatistico e regolazione amministrativa*, in corso di pubblicazione su “Munus” (si ringrazia l’Autore per aver consentito una lettura in anteprima)



DORINDA CACCIOPPO

***Sharenting* e tutela dei dati personali del minore: profili giuridici di un fenomeno interdisciplinare**

Il lavoro si propone di analizzare le implicazioni giuridiche del fenomeno dello “sharenting”. Partendo da una prospettiva interdisciplinare di descrizione della fenomenologia della questione si giunge, quindi, all’approfondimento dei profili giuridici riguardanti la protezione dei dati personali e la tutela dei diritti fondamentali del minore. Si dà quindi conto dello stato dell’arte attuale della disciplina normativa sullo “sharenting” in Italia e in Francia per poi trarre alcune considerazioni sul rapporto tra fatti e regolamentazione.

Sharenting – Data protection – Educazione digitale

Sharenting and children's data protection: legal aspects of an interdisciplinary phenomenon

The paper sets out to analyse the legal implications of the phenomenon of ‘sharenting’. Starting from an interdisciplinary perspective of description of the phenomenology of the issue, it then comes to an in-depth examination of the legal profiles concerning the protection of personal data and the protection of the fundamental rights of minors. The current state of the art of the regulatory framework on ‘sharenting’ in Italy and France is then discussed, followed by some considerations on the relationship between facts and regulation.

Sharenting – Data Protection – Digital Education

L’Autrice è dottoranda di ricerca in Istituzioni di diritto pubblico presso l’Università degli Studi Roma Tre

Questo contributo fa parte della sezione monografica *Minori e Internet* a cura di Carlo Colapietro e Antonio Iannuzzi

SOMMARIO: 1. La condivisione online dei minori: un dialogo tra diritto e neorealismo cinematografico. – 2. I termini della questione: il fenomeno dello *sharenting* e dei *baby influencers*. – 3. La questione giuridica della protezione dei dati personali dei minori: i limiti del consenso informato dei genitori. – 4. Riferimenti normativi dello *sharenting*: le proposte legislative in Italia. – 5. Il paradigma delle leggi francesi. – 6. Qualche considerazione sul rapporto tra fatti e regolamentazione.

1. La condivisione online dei minori: un dialogo tra diritto e neorealismo cinematografico

L'analisi del fenomeno dello *sharenting*, come pratica di condivisione online da parte dei genitori di materiali audio visivi aventi come protagonisti i propri figli, ha bisogno di un metodo d'esame che tenga conto della sua intrinseca natura interdisciplinare.

Ciò è ancor più evidente ove si consideri che tale questione si inserisce in un contesto sociale in cui la comunità virtuale ha assunto un rilievo prevalente dal punto di vista psicologico, in alcuni casi dal punto di vista lavorativo, più generalmente in una prospettiva economica e, dunque, giuridica. La narrazione costante della vita quotidiana attraverso le piattaforme digitali – mantenendo una patina di finzione omologante – risponde alle esigenze di appartenenza, di riconoscimento e alla necessità di autorealizzazione¹ (generalmente

vengono pubblicati contenuti audiovisivi sui traguardi raggiunti nella vita personale e lavorativa) della quasi totalità degli individui nella propria comunità di riferimento ma anche, in molti casi, a livello globale.

Tale commistione tra vita privata e mondo definibile (pur con una generalizzazione) “audio-visivo” sembra avviare un “dialogo impossibile” tra le varie discipline, fino a far comunicare, ad esempio, il contesto culturale del cinema con il diritto. Infatti, spostando la prospettiva sulle aspirazioni umane descritte, ora alla base del contemporaneo *social sharing*, si osserva come queste ultime fossero già state colte dal neorealismo cinematografico². Tale poetica cinematografica voleva raccontare la quotidianità contemporanea di persone vere, a volte quasi con un «pedinamento»³ del personaggio della vita comune; una tipologia di materiale che, agli occhi di un osservatore odierno, costituisce la base dell'identità e del ruolo digitale di

1. Si prende spunto dalle fasi della *Piramide dei bisogni* ideata nel 1954 dallo psicologo statunitense Abraham Maslow. La Piramide voleva essere una rappresentazione delle fasi che un essere umano affronta per raggiungere la propria realizzazione. Si partiva da una base di bisogno fisiologico, cioè legato alla sopravvivenza fisica e all'autoconservazione (fame, sete, sonno, termoregolazione, ecc.); al gradino superiore il bisogno di sicurezza, connesso alla garanzia per l'individuo di protezione e ragionevole tranquillità; al livello ancora superiore il bisogno di appartenenza costituito dall'aspirazione dell'individuo di essere parte di una comunità; quindi, il bisogno di stima, che porta con sé le esigenze di riconoscimento e approvazione; in cima alla Piramide il bisogno di autorealizzazione, in cui tutte le aspettative, le potenzialità si riuniscono nell'affermazione di un'identità e di un ruolo sociale.
2. Voce *Neorealismo - Cinema*, in “Enciclopedia Treccani” online.
3. PAGNI 2014, p. 12. L'A. parla della tecnica di Cesare Zavattini, il quale basava la sua narrazione sul pedinamento della persona semplice, pur sempre personaggio, nei momenti comuni della sua vita, attingendo spesso anche da fatti di cronaca.

un gran numero di persone. Proprio a questa corrente appartiene un soggetto di Cesare Zavattini, uno dei padri del neorealismo, che rappresenta – a parere di chi scrive – uno di quei casi in cui la rappresentazione artistica libera, parlando d'altro, anticipa problemi futuri, come ad esempio quello dello *sharenting*, e suggerisce alle altre discipline – tra cui il diritto – i valori alla base di una regolamentazione di fenomeni che continueranno a ripresentarsi in forme diverse nell'evoluzione storica dell'uomo: “Bellissima”⁴. Una madre desiderosa di far diventare la sua bambina ricca e famosa la espone alle telecamere acconciata e ammaestrata secondo le richieste. Verso la conclusione dell'iter di scelta delle bambine da ingaggiare (e del film) il regista mostra i selezionatori in una stanza che si divertono deridendo il video della bambina in lacrime e disperata per lo stress dell'esposizione ai ritmi delle riprese. La madre cerca di giustificare le risate sperando che l'ilarità possa comunque sortire l'effetto desiderato di far scegliere dal pubblico la sua bambina tra tante, poi – spinta dall'umiliazione e dalla volontà di tutelare sua figlia – rifiuta la possibilità di stipulare qualsiasi tipo di contratto in suo nome.

Il problema dell'eccessiva o della scorretta esposizione dei minori non è un fenomeno nuovo, prima riguardava riviste, poi il cinema, la televisione e ora, per via del funzionamento delle piattaforme social e in generale di Internet⁵, ha invaso la sfera intima della quotidianità.

Pertanto, le immagini del film descritte, sembrano offrire gli elementi base da tenere in considerazione per svolgere un'analisi di diritto del fenomeno dello *sharenting*, dell'*oversharenting* e di conseguenza della proliferazione dei c.d. *baby influencers*: l'attività dell'esposizione mediatica del minore con le sue conseguenze sull'individuo minore, il problema del grado di informazione del

consenso del genitore, le possibili derive dell'esposizione – pur consensuale – a terzi.

Dunque, il diritto può scegliere due strade per garantire una tutela sostanziale dei diritti e delle libertà dei minori esposti alle piattaforme digitali e al Web. Una prima strada è quella del divieto indiscriminato in un'ottica sanzionatoria e repressiva. La strada alternativa è quella di una regolamentazione che ponga limiti ma insista sull'educazione, sull'informazione e sulla sensibilizzazione. In altri termini, una concreta formazione degli adulti (anche in quanto genitori o esercenti la responsabilità genitoriale) ad un utilizzo consapevole delle modalità di esposizione dei minori sulle piattaforme digitali. Quest'ottica, pur correndo il rischio per alcuni tratti di prendere una deriva paternalistica, se ne allontana distintamente mirando a garantire, nella sostanza, il diritto ad una cittadinanza consapevole (anche, ma non solo, digitale).

2. I termini della questione: il fenomeno dello *sharenting* e dei *baby influencers*

L'Oxford English Dictionary fa risalire al 2010 un primo isolato utilizzo del termine *sharenting* come azione di condivisione delle responsabilità di essere un genitore o un *caregiver*.

È poi nel 2012 che Steven Leckart, utilizzando il termine *oversharenting* in un suo articolo per il Wall Street Journal⁶, permette di stabilizzare per deduzione un significato comune del termine: l'azione o la pratica di condividere notizie, immagini o video dei propri figli sui «social media websites»⁷.

La questione dello *sharenting* ha più livelli, che giungono tutti a questioni giuridiche, per alcuni tratti, analoghe ma è necessario distinguerne la fenomenologia proprio per comprendere la natura e il livello di dettaglio dei possibili presidi giuridici che dovrebbero venire in rilievo.

4. Poi divenuto, nel 1951, l'omonimo film di Luchino Visconti. Disponibile interamente su Youtube.

5. GRISWOLD 2012. L'A. osserva come Internet, infatti, più che modificare le pratiche culturali già esistenti, ne agevola la riproduzione e co-costruzione.

6. LECKART 2012. L'A. scrive: «I call it “oversharenting”: the tendency for parents to share a lot of information and photos of their kids online».

7. «The action or practice of sharing news, images, or videos of one's children on social media websites» voce *Sharenting*, in “Oxford English Dictionary”.

Vi è una prima fattispecie in cui un genitore, senza scopi commerciali, per mera fierezza⁸ o per emulazione⁹, cui a volte si accompagna una conoscenza parziale del complessivo funzionamento delle piattaforme e delle possibili conseguenze della pubblicazione di contenuti, pubblica foto dei propri figli: nel caso definito da Leckart in quantità eccessive (c.d. *oversharenting*) o altrimenti in situazioni in cui sarebbe inopportuno.

Vi è poi una seconda possibile fattispecie in cui un genitore pubblica contenuti aventi come protagonisti minori per finalità prevalentemente commerciali. Il minore, tendenzialmente, diviene un mezzo di validazione sulle piattaforme social, in grado di generare un tasso di interazione¹⁰ molto alto. A questa fattispecie appartiene anche il fenomeno dei *baby influencer*: si tratta di minori che accedono, con l'aiuto dei genitori, prima dell'età minima per l'iscrizione fissata a 14 anni, all'ambiente digitale pubblicando contenuti fino, talvolta, a ricevere contratti di sponsorizzazione per la promozione di prodotti e marchi.

Si può poi individuare una terza fattispecie (che in alcuni casi costituisce una variazione della seconda fattispecie descritta): il genitore che pubblica contenuti aventi come protagonisti i minori è già un *influencer*; la pubblicazione di foto e video dei figli minori, a partire dalle prime

ecografie, è parte del suo lavoro di creazione dei contenuti.

Le questioni giuridiche relative a questi fenomeni sono variegate. Se ne proverà a fare una introduttiva sistematizzazione per poi approfondire gli ambiti problematici legati alla protezione dei dati personali e ai profili costituzionali.

Il primo e più rilevante aspetto critico comune a tutte e tre le fattispecie è la creazione di un'identità digitale del minore, con una conseguente reputazione online¹¹, senza che quest'ultimo possa prestare un effettivo consenso informato. Questa situazione potrebbe comportare, dunque, l'eventuale necessità per il minore, una volta maggiorenne, di esercitare il diritto all'oblio perché possa essergli restituito l'anonimato.

Rileva, inoltre, in maniera condivisa da tutte e tre le fattispecie descritte, il problema della contenutizzazione secondaria¹², un problema che va ben oltre i contenuti, talvolta sessualizzati¹³, pubblicati online dai genitori o in alcuni casi dagli stessi minori: foto, audio e video riguardanti minori, pubblicati con e senza scopo commerciale, possono essere presi e utilizzati per creare contenuti di tipo diverso e con un diverso grado di interazione, finanche esponendo le immagini e i video dei minori a diventare materiale pedopornografico¹⁴. Proprio quest'ultimo rischio è

8. LECKART 2012, «Proud parents have been perfecting this genre for decades. While the intimate moments themselves remain largely unchanged, how we choose to share them – much like the tools for capturing them – has evolved dramatically [...]».

9. Fenomeno tipico nell'utilizzo delle piattaforme social.

10. L'*engagement rate* o tasso d'interazione è un sistema di misurazione del livello di coinvolgimento degli utenti con i contenuti digitali che include *like*, commenti, condivisioni e clic. Il fatto che contenuti di minori generino un livello superiore di interazione apre un ulteriore problema relativo alla tipologia dei meccanismi di visibilità di queste infrastrutture tecnologiche.

11. Cfr. DOCKTERMAN 2013.

12. MEAKIN 2013.

13. Per contenuti sessualizzati si intendono quelli in cui i minori mangiano, assumono pose, emettono suoni che, al percepito di un adulto, possono facilmente ricondursi e ammiccare alla sfera sessuale.

14. Tribunale civile Trani, ord. 7 settembre 2021 (minori e social network). Nell'ambito di un procedimento instaurato ex art. 700 c.p.c. dal padre di una bimba minore al fine di ottenere la rimozione delle foto della figlia pubblicate sui social network dalla madre senza il suo consenso, il Tribunale, richiamando precedente giurisprudenza di merito, osserva come l'inserimento di foto di minori sui social network costituisca comportamento potenzialmente pregiudizievole per essi in quanto ciò determina la diffusione delle immagini fra un numero indeterminato di persone, conosciute e non, le quali possono essere malintenzionate e avvicinarsi ai bambini dopo averli visti più volte in foto online, non potendo inoltre andare sottaciuto l'ulteriore pericolo costituito dalla condotta di soggetti che taggano le foto online dei minori e, con procedimenti di fotomontaggio, ne traggono

attualmente sempre più concreto data la diffusione dell'impiego di intelligenze artificiali per generare materiale pornografico spacciato per reale ma, in realtà, realizzato combinando immagini di soggetti pubblicate online e immagini pornografiche, i c.d. “*deep fake porn*”¹⁵.

Dal punto di vista costituzionalistico, diversi sono gli aspetti del fenomeno dello *sharenting* che stridono con la complessiva tutela costruita attorno al minore dall'art. 30 Cost. e, nel dettaglio, dal c.d. «statuto dei diritti del figlio»¹⁶ ex art. 315-bis del Codice civile. Altresì, viene in rilievo il concetto di dignità della persona in quanto tale come solido fondamento del diritto all'identità personale: i contenuti che vengono esposti generalmente dai genitori al fine di generare facili ilarità – ancor peggio nei casi dei contenuti sessualizzati – con lo scopo di aumentare le interazioni e le visualizzazioni sulle piattaforme social o ancora al fine di sponsorizzare un prodotto o un servizio – come ne caso dei *baby influencers* – rischiano di minare non solo la dignità del minore ma anche la sua capacità di costruirla e concepirla nel corso del suo sviluppo.

Nel caso dei *baby influencers* si pone anche il problema di capire in che termini si possa (o si debba?) parlare di sfruttamento del lavoro minorile. In generale, il lavoro minorile, inteso come lavoro dei minori di quindici anni e degli adolescenti fino ai diciotto anni, è regolato dalla legge 17 ottobre 1967, n. 977. Il limite dei sedici anni per la capacità giuridica in ambito giuslavoristico è derogabile solo per attività lavorative di carattere culturale, dello spettacolo che, ad ogni modo, sono subordinate all'ottenimento dell'autorizzazione dell'ispettorato del lavoro e alla garanzia dell'integrità psico-fisica e dello sviluppo dei minori. Il consenso congiunto di entrambi i genitori è solo uno dei requisiti

necessari; nell'attuale fenomeno dei *baby influencers*, invece, rappresenta l'unico requisito rispettato nella prassi.

3. La questione giuridica della protezione dei dati personali dei minori: i limiti del consenso informato dei genitori

Ai fini della ricerca, nell'ambito del diritto alla protezione dei dati personali europeo in materia si possono separare due aree di rilievo: una prima area che riguarda la tutela dei dati personali del minore che mira a rafforzare il controllo e a richiedere il consenso di chi ha la responsabilità genitoriale; una seconda area, non ancora normativamente disciplinata ma parzialmente inquadrata in via pretoria, che riguarda tutte le conseguenze sui minori di quel consenso.

Per quanto attiene alla prima area di interesse, un preliminare sguardo d'insieme rivela come il contesto normativo antecedente al GDPR non prevedesse una disciplina specifica per il trattamento dei dati dei minori nella dimensione online. Il regolamento riconosce, dunque, al minore il suo carattere di soggetto vulnerabile e al trattamento dei suoi dati la natura di fattore di incremento dei rischi per i diritti e le libertà delle persone fisiche¹⁷. Il GDPR, infatti, inserisce i minori nel nuovo impianto sistematico introducendo alcuni cambiamenti significativi di dettaglio della disciplina, quali – ad esempio – l'obbligo di verificare l'età dell'utilizzatore dei servizi della società dell'informazione nonché la prestazione del consenso dei genitori (o in ogni caso degli esercenti la responsabilità genitoriale) per l'accesso dei figli minori ai suddetti servizi.

Ad incrementare queste tutele devono poi aggiungersi quelle previste dalla Direttiva (UE)

materiale pedopornografico da far circolare fra gli interessati. Dunque, il pregiudizio per il minore è insito nella diffusione della sua immagine sui social network.

15. Su questo tema molto interessante è la disamina operata in BELISARIO-RICCIULLI 2024, in cui si approfondisce il caso della Corea del Sud ove «nel 2022, un centro di supporto digitale per i reati sessuali gestito dall'amministrazione metropolitana di Seul ha sviluppato uno strumento in grado di tracciare, monitorare ed eliminare automaticamente immagini e video *deepfake* 24 ore su 24. La tecnologia, che ha vinto il premio UN Public Administration Prize 2024, ha contribuito a ridurre il tempo impiegato per trovare i *deepfake* da una media di due ore a tre minuti. Tuttavia, sebbene tali tentativi possano aiutare a ridurre ulteriori danni causati dai *deepfake*, è improbabile che siano soluzioni definitive».

16. CARRANO 2011.

17. Considerando 75 GDPR.

2010/13 nota come Direttiva europea sui servizi media audiovisivi (AVMSD), revisionata nel 2018, sugli obblighi relativi alle misure idonee alla tutela dei minori da contenuti online nocivi, nonché dal Digital Services Act (DSA) che inserisce la tutela dei minori nel generale obiettivo di contrasto attivo alla diffusione online di contenuti illeciti e dei rischi connessi all'utilizzo improprio dei servizi digitali¹⁸.

Entrando più nel dettaglio del Regolamento 679/2016, l'art. 8 prevede che un trattamento di dati operato nel contesto di offerte di servizi della società dell'informazione dirette a minori è lecito solo ove il minore abbia almeno 16 anni (pur potendo gli Stati membri stabilire un'età inferiore ma non al di sotto dei 13 anni).

In Italia, l'art. 2-*quiquies* del d.lgs. 101/2018, che ha adeguato il d.lgs. 196/2003 (Codice privacy) al GDPR, ha portato a 14 anni l'età minima per il c.d. consenso digitale e ha esplicitato l'accessibilità, la comprensibilità e la chiarezza che devono caratterizzare il linguaggio dell'informativa predisposta dal titolare per l'offerta diretta al minore. Una tutela specifica dovuta alla circostanza per cui i minori «possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali»¹⁹. Il Comitato europeo per la protezione dei dati, nel 2020²⁰, ha elaborato un aggiornamento delle Linee guida sul consenso riservando una particolare attenzione al consenso dei minori che accedono ai servizi dell'informazione per cui il titolare del trattamento, nel verificare la validità del consenso prestato dal minore, è chiamato a «compiere ogni ragionevole sforzo per verificare che l'utente abbia raggiunto l'età del

consenso digitale, e le misure dovrebbero essere proporzionate alla natura e ai rischi delle attività di trattamento».

Il *favor minoris*²¹ espresso dall'art. 8 GDPR ispira diversi altri riferimenti normativi: l'art. 12, par. 1 GDPR esprime il dovere di rendere accessibile e comprensibile l'informativa destinata ai minori secondo le loro capacità cognitive, utilizzando un linguaggio «semplice e chiaro che un minore possa capire facilmente»²² per qualsiasi informazione e comunicazione a loro rivolta; l'art. 17, par. 1 lett. f) GDPR sancisce il diritto alla cancellazione dei dati raccolti nel contesto della fornitura a minori di servizi della società dell'informazione, un diritto all'oblio di estremo rilievo se l'interessato ha fornito il suo consenso da minorenni²³ ponendo le basi della sua reputazione online futura. Ad ogni modo, per i minori al di sotto della maggiore età (quantomeno) digitale²⁴ il consenso deve essere prestato o autorizzato da chi esercita la responsabilità genitoriale.

Ed è proprio su questo punto che si entra nella seconda area di interesse per la ricerca: l'esercente la responsabilità genitoriale esprime il suo consenso in luogo del minore. Il suo consenso è specifico e informato sulle concrete conseguenze che potrebbe avere sul minore? La questione è di non poco momento poiché, quando si osservano le fattispecie dall'angolo visuale della protezione dei dati dei minori, il presupposto da cui si prendono le mosse sembra essere quello di un consenso del genitore necessariamente informato in quanto posto in una relazione asimmetrica con quello del minore vulnerabile. Tuttavia, proprio in questo passaggio logico si innesta l'esigenza di fondo da cui deve partire il legislatore nella costruzione di

18. Questa parte è esaminata nel contributo presente in questo volume da LUCARELLI TONINI 2024. Si riporta successivamente una bibliografia minima per approfondimento: COLAPIETRO-IANNUZZI 2017; OROFINO 2018; CORRIERO 2004; OROFINO 2023.

19. Considerando 38 GDPR.

20. EUROPEAN DATA PROTECTION BOARD 2020; BRAVO 2017.

21. RESTA 2022, p. 105 ss.

22. Considerando 58 GDPR.

23. Considerando 65 GDPR: «[...] tale diritto è in particolare rilevante se l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare tale tipo di dati personali, in particolare da internet. L'interessato dovrebbe poter esercitare tale diritto indipendentemente dal fatto che non sia più un minore [...]».

24. Espressione di AGOSTINELLI 2023. Anche detta «limitata capacità d'agire on-line» (RESTA 2022).

una regolamentazione e forse, soprattutto, nella preparazione di un terreno fertile (e informato) in cui tale regolamentazione possa trovare una sua realizzazione efficace e concreta.

Di qui, però, può sorgere un ulteriore quesito d'indagine: nel caso in cui – ben informato e consapevole dei rischi – il genitore decidesse di procedere con la prestazione del consenso e, come nel caso dello *sharenting*, con la diffusione anche pubblica dei dati del minore, esistono tutele effettive per quest'ultimo?

4. Riferimenti normativi dello *sharenting*: le proposte legislative in Italia

L'art. 30 della Costituzione prevede il dovere per il genitore di mantenere istruire ed educare i figli, un dovere che si concretizza ed emerge nella sostanza dall'art. 315-*bis* del Codice civile in cui si pone l'accento sui diritti che complessivamente compongono «un unico, globale e fondamentale diritto del minore ad ottenere in tutto il suo percorso formativo, sostegno, guida e protezione per strutturarsi adeguatamente come persona»²⁵. Questo insieme di tutele, unito all'art. 147 c.c. in cui viene esPLICITATO il rispetto necessario delle capacità, delle inclinazioni naturali e delle aspirazioni del figlio, si deve adattare al nuovo ambiente digitale. Dunque, gli obblighi relativi alla responsabilità genitoriale impongono di fornire un'educazione digitale idonea all'utilizzo dei mezzi della comunicazione ma anche di vigilare attivamente sulla quantità e sulla qualità della presenza dei minori su Internet per evitare il rischio di incidere negativamente sullo sviluppo psico-fisico del minore²⁶. Seguendo questa linea, in diverse pronunce giurisprudenziali

recenti, l'attività di diffusione sulle piattaforme digitali online di video e foto relativi ai minori è stata considerata un comportamento potenzialmente pregiudizievole²⁷ proprio per il rischio di diffusione incontrollata, arrivando in alcuni casi anche ad ordinarne la cessazione al genitore perpetrante²⁸.

Altresì, la diffusione incontrollata della quantità e qualità dei contenuti riguardanti i minori incide sulla dignità personale in quanto stabile elemento fondante il diritto all'identità personale *ex* artt. 2 e 3 della Costituzione. Il portato del fenomeno dello *sharenting*, quale invasione della sfera individuale nella paradossale costruzione eteronoma di un'identità digitale del minore, rischia di minare – in primo luogo – la capacità dello stesso di discernere la propria identità personale da quella digitale e – in secondo luogo – la capacità del minore di concepire la dignità in quanto valore anche nel corso del suo sviluppo. Il problema della definizione degli estremi qualificanti il valore della dignità riguarda sicuramente l'etica e la filosofia ma costituisce un dibattito interrogativo anche dal punto di vista costituzionale. Non potendo in questa sede approfondire i termini della questione²⁹, la chiave interpretativa a cui sembra opportuno far riferimento è quella che collega la concezione di dignità proprio alla costruzione dell'individualità. È, dunque, la Corte costituzionale in una pronuncia significativa, seppur risalente, ad osservare che «la sfera intima della coscienza individuale deve esser considerata come il riflesso giuridico più profondo dell'idea universale della dignità della persona umana»³⁰ e a precisare, qualche anno dopo, che «l'identità personale costituisce un bene per sé medesima, [...]

25. MORO 2014, p. 189; DI COSTANZO 2023.

26. Si cfr. Tribunale minorenni, Caltanissetta, 8 ottobre 2019 (in cui viene citata la pronuncia del Trib. di Teramo, 16 gennaio 2012, in cui si affronta il tema della responsabilità civile dei genitori ai sensi dell'art. 2048 c.c. nell'ipotesi di danno cagionato dal minore attraverso Facebook); Tribunale civile Parma, I sez., sentenza n. 698 del 2020 in cui si afferma che il diritto-dovere dei genitori di educare i propri figli racchiude anche l'educazione digitale dei minori. Soprattutto i contenuti presenti sui telefoni cellulari dei minori devono essere costantemente supervisionati da entrambi i genitori, anche se legalmente separati, al fine di prevenire ed evitare la comparsa di materiali non adatti all'età e alla formazione educativa dei minori. La stessa regola vale per l'utilizzo del computer, al quale andranno applicati i necessari dispositivi di filtro.

27. Tribunale civile Trani, ord., 30 agosto 2021; Tribunale civile Rieti, ord. 7 marzo 2019 n. 94488.

28. Tribunale civile Roma, sez. I, 23 dicembre 2017 n. 94149.

29. Si veda *ex multis* la ricostruzione complessiva di DOLSO 2019.

30. Corte cost., sent. n. 467 del 1991.

di guisa che a ciascuno è riconosciuto il diritto a che la sua individualità sia preservata»³¹.

Vieppiù, la questione dello *sharenting* è stata analizzata a livello nazionale e internazionale cercando di supportare con dati statistici l'entità del fenomeno³², inserendo opportunamente tra i fattori degni di rilievo anche una variabile assai frequente: il nesso dei fenomeni distorsivi della pubblicazione online delle foto dei minori con una scarsa educazione digitale dell'adulto.

Proprio per guidare il contenimento di questa deriva informativa il Garante per la protezione dei dati personali si è pronunciato in molte occasioni per definire i termini del problema dello *sharenting*³³ fornendo anche un *vademecum* che restituisse icasticamente le maggiori criticità della relazione dei minori con le nuove tecnologie e che desse dei

«consigli ai “grandi” per un utilizzo sicuro da parte dei “piccoli”»³⁴.

Con la fondamentale partecipazione delle autorità amministrative indipendenti competenti (tra cui lo stesso GPDP, l'AgCOM, l'Agia), nel 2021 il Ministero della Giustizia ha istituito un tavolo tecnico dedicato al tema dei minori nell'interazione con i social network. Dal report di risulta emergono temi come l'*age verification*, il fenomeno dei cc.dd. *baby influencers* ma soprattutto l'esigenza, trasversale ad ogni questione, di promuovere campagne efficaci di sensibilizzazione ed educazione ai rischi del Web.

Il tema continua ad essere oggetto di un fervente e partecipato dibattito che ha portato tra il 2023 e il 2024 alla presentazione di quattro proposte di legge³⁵ differenti volte al tentativo di cristallizzare

31. Corte cost., sent. n. 13 del 1994.

32. Nel testo della proposta di legge (che si approfondirà a seguire nel corpo del testo) n. 1771 del 12 marzo 2024 sullo *sharenting*, “Modifiche alla legge 17 ottobre 1967, n. 977, in materia di impiego dei minori nell'ambito delle piattaforme digitali di condivisione di contenuti multimediali, nonché disposizioni sulla diffusione dell'immagine e di contenuti multimediali di minori” vengono riportati alcuni dati significativi: «Nel 2016, una ricerca dell'organizzazione inglese The Parent Zone ha rivelato che i genitori pubblicano quasi millecinquecento foto dei figli prima che questi compiano cinque anni, con una media di circa trecento immagini all'anno. E già nel 2013 il quotidiano irlandese Irish Examiner segnalava che le foto di più di due terzi dei neonati vengono diffuse on line entro un'ora dal parto (per l'esattezza, 57,9 minuti). In uno studio italiano, pubblicato a fine 2017 sulla Rivista italiana di educazione familiare, si attesta che l'88 per cento delle mamme che pubblica le foto dei figli ha dichiarato di aver impostato le opzioni di privacy in modo da limitare la cerchia di persone che possono visualizzare i contenuti. Nell'83 per cento dei casi è stata selezionata l'opzione che estende la condivisione ai soli amici, dunque senza alcuna limitazione significativa. Il fenomeno sembra più diffuso per i piccoli, da zero a tre anni, le cui immagini sono condivise dall'86 per cento dei genitori, e tende poi a diminuire con l'età dei figli medesimi. Nel 2021, secondo i dati raccolti dalla società Security.org il 77 per cento dei genitori ha condiviso storie, video o immagini dei figli sui social media (nell'80 per cento dei casi ciò è avvenuto con l'indicazione dei veri nomi dei minori). Un dato confermato da un'analisi pubblicata già nel 2020 dal centro studi Pew Research secondo cui l'82 per cento dei genitori che utilizzano i social media pubblica foto, video o altre informazioni sui propri figli. Secondo la Barclays Bank, il caricamento indiscriminato di contenuti multimediali concernenti i bambini sarà la causa dei due terzi dei furti di identità che i giovani dovranno affrontare entro la fine del decennio, ovvero 7,4 milioni di questi eventi ogni anno entro il 2030, per un costo di 667 milioni di sterline l'anno». Interessanti sono anche i dati riportati in questa [ricerca della società benefit inglese Nominet](#).

33. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI S.d.

34. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI 2021.

35. Proposta di legge n. 1771/2024, presentata il 12 marzo 2024, Sportiello, “Modifiche alla legge 17 ottobre 1967, n. 977, in materia di impiego dei minori nell'ambito delle piattaforme digitali di condivisione di contenuti multimediali, nonché disposizioni sulla diffusione dell'immagine e di contenuti multimediali di minori”; proposta di legge n. 1800/2024, presentata il 22 marzo 2024, Bonelli et al., “Modifiche all'articolo 37 del testo unico dei servizi di media audiovisivi, di cui al decreto legislativo 8 novembre 2021, n. 208, in materia di impiego dei minori nell'ambito delle piattaforme digitali per la condivisione di video, audio e immagini, e disposizioni concernenti il diritto del minorenne alla rimozione dei dati e dei contenuti che lo riguardano dalla rete internet e dai motori

una tutela effettiva per il minore che utilizza o è utilizzato come contenuto digitale su una piattaforma digitale e, in generale, su Internet.

La proposta di legge n. 1771/2024 interviene con cinque articoli sulla legge n. 977/1967 per regolare alcuni aspetti della partecipazione “funzionale” dei minori nelle piattaforme digitali introducendo, ad esempio, delle tutele giuslavoristiche: l’art. 4bis stabilisce che per il minore impiegato sulle piattaforme digitali debba essere stipulato un contratto di lavoro. La direzione provinciale deve aver autorizzato l’attività e l’autorizzazione (semestrale) deve essere sottoposta a periodico riesame. Altresì, nel caso di autorizzazione dei minori di quindici anni, la direzione provinciale è tenuta a fornire agli esercenti la responsabilità genitoriale e, a chi impiega il minore, il dettaglio delle informazioni sulla tutela dei diritti del minore, sulle conseguenze nella vita privata del minore e degli adempimenti finanziari attinenti ai proventi delle attività del minore. Viene previsto, infatti, un conto corrente gestito, fino ai diciotto anni del minore, da un curatore speciale nominato dal tribunale.

Si interviene, dunque, in maniera specifica sul fenomeno dello *sharenting* cercando di consolidare un sistema complessivo di tutele sulla diffusione dell’immagine dei minori nonché sui diritti di cancellazione dei dati del minore stesso. Viene previsto, infatti, il diritto all’oblio del minore che, una volta compiuti i quattordici anni, può in ogni momento richiedere la cancellazione dei dati personali, anche in relazione ai contenuti multimediali diffusi da chi ha la responsabilità genitoriale o con il suo consenso.

La tutela del diritto alla riservatezza acquisisce maggior concretezza nel divieto di diffusione di notizie o contenuti multimediali riguardanti i minori senza che ciò sia nell’interesse primario e oggettivo del minore, richiamando così i principi e i limiti stabiliti dalla Carta di Treviso³⁶. Il consenso prestato dai genitori deve tenere conto in ogni caso della volontà espressa del minore, gli esercenti la responsabilità genitoriale devono renderlo partecipe nell’esercizio dei suoi diritti di immagine parametrandone il coinvolgimento all’età nonché al grado di maturità³⁷. Per quanto riguarda le piattaforme digitali, a queste ultime è richiesta l’adozione di un codice di regolamentazione concordato con le Autorità³⁸. Da ultimo, un particolare rilievo viene dato alla necessità di istituire campagne informative periodiche di prevenzione e sensibilizzazione sulla complessità dei fenomeni dei *baby influencer* e dello *sharenting*.

La prospettiva della proposta di legge n. 1800/2024, pur condividendo molte delle misure previste dalla proposta n. 1771/2024, si rivolge a tali fenomeni ponendo in capo a chi esercita la responsabilità genitoriale l’obbligo di dichiarare all’Autorità per le garanzie nelle comunicazioni (AGCOM) l’attività di diffusione di qualunque tipo di contenuto che riguardi un minore di quattordici anni tramite servizi di piattaforma per la condivisione di video, audio o immagini.

La proposta di legge bipartisan del Senato n. 1863/2024 aggiunge alle garanzie descritte negli altri testi presentati alcuni obblighi in capo ai fornitori di servizi della società dell’informazione: ad esempio, l’art. 6 descrive la necessità di attivare

di ricerca”; proposta di legge n. 1863/2024, presentata il 13 maggio 2024, Madia - Mennuni, “Disposizioni per la tutela dei bambini e degli adolescenti nell’utilizzo degli strumenti digitali”; proposta di legge n. 1217/2024, presentata l’8 giugno 2023 ma l’esame in Commissione è iniziato il 26 giugno 2024, “Modifiche al codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, in materia di verifica dell’età degli utenti dei servizi di comunicazione elettronica, e altre disposizioni per la tutela dei minori nella fruizione di tali servizi”.

36. La *Carta di Treviso*, protocollo condiviso tra Ordine dei giornalisti, Federazione nazionale della stampa italiana e Telefono azzurro (firmato il 5 ottobre 1990) si propone di disciplinare i rapporti tra informazione e infanzia. La Carta vuole operare un equo bilanciamento tra diritto di cronaca e responsabilità dei mezzi d’informazione rispetto all’immagine dei minori. Interessi in gioco sono l’identità, la personalità e la concreta tutela dei diritti dei minori.

37. Ciò nel rispetto degli articoli 10 e 320 del codice civile, degli articoli 96 e 97 della legge sul diritto d’autore n. 633 del 1941. e della Convenzione delle Nazioni Unite del 1989.

38. Nello specifico: l’Autorità per le garanzie nelle comunicazioni, il Garante per l’infanzia e l’adolescenza, il Garante per la protezione dei dati personali e il Comitato di applicazione del codice di autoregolamentazione media e minori.

una funzionalità «che consenta ai minori di anni quindici l'attivazione istantanea di un canale di comunicazione vocale o testuale con il numero di emergenza per l'infanzia "114"». Viene proposta, poi, l'abrogazione del comma 1 dell'articolo 2-*quinqies* del Codice Privacy riguardante il consenso digitale del minore che abbia compiuto i 14 anni.

L'ultima proposta qui citata è in realtà la più risalente, presentata alla Camera l'8 giugno 2023, a giugno 2024 approdata per l'esame in Commissione e recante modifiche al Codice Privacy in materia di verifica dell'età degli utenti dei servizi di comunicazione elettronica. La proposta, pur essendo prevalentemente indirizzata ai mezzi di *age verification*, condivide con le successive precedentemente descritte il rilievo attribuito alle campagne informative di sensibilizzazione sull'uso consapevole dei servizi di comunicazione sociale.

5. Il paradigma delle leggi francesi

Le proposte di legge italiane prendono le mosse dalla legge francese n. 120 del 19 febbraio 2024 volta a garantire il rispetto del diritto all'immagine dei minori. L'anno precedente era stata depositata, presso l'Assemblea Nazionale, la proposta n. 758/2023³⁹ che sollevava la necessità di regolamentare la condivisione online delle immagini dei minori. In questa istanza confluivano temi come lo sfruttamento commerciale del minore, la questione della criminalità minorile nonché i rischi dell'esposizione mediatica del minore nei confronti della sua integrità psico-fisica.

Il problema della longevità dei dati che «si ritrovano immortalati nei sedimenti del cyberspazio»⁴⁰ non poteva non far emergere, da un lato, il rischio dell'adescamento con finalità di pedofilia, del cyberbullismo, della lesione della dignità del minore cui viene attribuita un'identità digitale non scelta e, dall'altro, l'urgenza di una regolamentazione che ponesse almeno parte degli argini necessari

a contenere le derive dei fenomeni dello *sharenting* e dei *baby influencer*.

Per quanto riguarda il secondo fenomeno, la Francia già nell'ottobre del 2020⁴¹ aveva adottato una legge che si occupava della disciplina dello sfruttamento commerciale dell'immagine dei minori di sedici anni sulle piattaforme online intervenendo sul codice del lavoro francese in maniera analoga a quanto ripreso poi dalle proposte normative italiane analizzate: l'attività dei *baby influencer* è riconosciuta quale lavoro minorile, vengono previste autorizzazioni al lavoro dalle autorità pubbliche locali e conti correnti intestati ai minori per gestire gli introiti derivanti dalle singole prestazioni; in chiusura al sistema delineato viene tutelato il diritto all'oblio del minore che richieda la rimozione dei contenuti, lavorativi o meno, che lo riguardano. In quest'ultimo aspetto si ritrova uno dei punti di contatto con la disciplina necessaria in materia di *sharenting*.

La legge francese sullo *sharenting* del febbraio 2024 pone al centro del quadro giuridico per la tutela dei diritti di immagine dei minori la responsabilità genitoriale. Sono, in primo luogo, gli esercenti la responsabilità genitoriale a dover tutelare l'interesse superiore del figlio minore, l'autorità pubblica deve poter intervenire solo in ultima istanza. Di qui l'importanza di una legge che privilegi l'educazione alla penalizzazione rispetto alla pubblicazione delle immagini dei minori online⁴².

Dunque, le modifiche al Codice civile francese prevedono l'introduzione della nozione di vita privata del figlio minore nella definizione di responsabilità genitoriale, l'applicazione della co-genitorialità nell'esercizio dei diritti di immagine del minore e la possibilità di delegare "*l'autorité parentale*" in caso di uso abusivo dell'immagine del minore. Viene modificata, in ultimo, la disciplina della protezione dei dati personali rafforzando i poteri della *Commission nationale de l'informatique et des libertés* (CNIL) in caso di pregiudizio minacciato o arrecato ai diritti e alle libertà dei

39. 16^e législature - [Proposition de loi visant à garantir le respect du droit à l'image des enfants, n° 758](#), déposée le jeudi 19 janvier 2023.

40. *Ibidem*.

41. Loi n. 2020-1266 du 19 octobre 2020 visant à encadrer l'exploitation commerciale de l'image d'enfants de moins de seize ans sur les plateformes en ligne.

42. HERVIEU 2024.

minori. Già in virtù dell'art. 21 della legge n. 78-17 del 6 gennaio 1978⁴³ la Commissione può, in caso di violazione, limitare temporaneamente e permanentemente il trattamento dei dati personali interessati; se le violazioni sono gravi ed immediate «il presidente della Commissione può anche chiedere, con procedimento sommario, al tribunale competente di ordinare, se necessario sotto pena, ogni misura necessaria alla tutela di tali diritti». e libertà⁴⁴. A seguito di questa recente riforma, la CNIL può ricorrere alla procedura sommaria d'urgenza descritta nel caso in cui venga violato il diritto d'immagine del minore, previa fissazione di criteri relativi alla gravità e all'immediatezza della violazione.

La normativa francese è stata considerata un modello capofila poiché riconosce uno spessore autonomo al minore nell'ambito della sua consueta subordinazione alla volontà degli esercenti la responsabilità genitoriale, quantomeno per la condivisione dei contenuti digitali. Questa esplicitazione ha, di certo, un valore comprensibile nel tempo al minore ma riveste un ruolo fondamentale nell'opera di responsabilizzazione ed educazione digitale degli individui, genitori o meno. Dunque, emerge con forza come non si possa più prendere le mosse dal presupposto del consenso del genitore come consenso necessariamente informato.

Infatti, la condizione di realizzazione dell'effettività della disciplina francese (così come di quella potenziale delle proposte italiane) è proprio l'investimento in campagne di informazione e sensibilizzazione che possano assottigliare le distanze tra le dinamiche del "fattore umano" e la costante evoluzione dell'innovazione tecnologica.

6. Qualche considerazione sul rapporto tra fatti e regolamentazione

I casi di *sharenting* considerabile "patologico" in maniera indiscussa sono ormai molteplici e di respiro globale. Il primo passo per giungere ad un'equa ed efficace regolamentazione è sicuramente quello di riuscire a porsi tutte le domande

necessarie per includere nella disciplina normativa un quantitativo di risposte quantomeno sufficienti a garantire la tutela dei diritti fondamentali e delle libertà in gioco.

Viene qui in rilievo, dunque, il caso americano di Ruby Franke, una mamma *youtuber* dello Utah conosciuta in rete con il canale "8 Passenger" attraverso il quale condivideva la sua vita familiare e offriva consigli sulla genitorialità. Nell'agosto del 2023 venne arrestata dopo che uno dei suoi figli, dodicenne, scappò di casa chiedendo aiuto ai vicini. La donna, a dicembre 2023, si è dichiarata colpevole di abusi e maltrattamenti sui minori relativi specificamente alle attività da *influencer*, al lavoro, quindi, che la donna richiedeva anche ai figli minori per mantenere alto il livello di interazione con il suo profilo⁴⁵.

Il 16 ottobre 2024 una delle sue figlie, Shari Franke, è stata audita dal Senato dello Utah⁴⁶ per fornire la sua testimonianza di figlia divenuta un asset, pur regolarmente contrattualizzato dai terzi cui offriva servizi di sponsorizzazione, del lavoro di creazione di contenuti digitali della madre⁴⁷. Il suo intervento, dichiara, ha il solo intento di «portare alla luce le problematiche etiche ed economiche che derivano dall'essere una bambina influencer»⁴⁸.

Anche con una prima analisi di superficie può essere utile ricostruire qualche cenno esemplificativo di un dialogo tra i fatti e le istanze delineate nelle proposte normative italiane basate sul paradigma francese.

Dall'audizione della ragazza emerge come la tutela giuslavoristica del minore può porre solo in parte un argine ad un fenomeno molto più ampio che pervade diversi ambiti della vita del minore stesso utilizzato come "contenuto digitale". Il problema della contrattualizzazione del lavoro svolto per il genitore parte dal rischio di fondo della difficoltà del far emergere di per sé l'attività lavorativa, soprattutto quando per garantire il proficuo funzionamento dell'*account* quello che viene richiesto al minore è farsi riprendere in un momento

43. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

44. Art. 21, Loi n° 78-17 du 6 janvier 1978.

45. Da un [editoriale](#) del Fatto Quotidiano del 21 febbraio 2024.

46. Nello Utah è in discussione una vera e propria riforma normativa per limitare l'esposizione dei minori ai social.

47. KINDELAN 2024.

48. Alcuni stralci rilevanti dell'audizione sono disponibili su [Youtube](#).

imbarazzante o emozionante (così come testimoniato da Shari Franke). D'altra parte, la proposta del testo italiano n. 1863/2024 di attivare un canale semplificato di comunicazione vocale o testuale con il numero di emergenza per l'infanzia, invece, sembra poter essere una tutela aggiuntiva efficace nella veste di misura normativa concreta, idonea a sostituire la fuga fisica dalla casa avvenuta, invece, in questo caso di cronaca.

Da ultimo, in chiosa alle questioni più di dettaglio, sembra potersi ritenere generalmente che le

campagne informative e formative generalizzate su questi temi, così come intese da tutti i testi normativi considerati, possano essere uno strumento efficace di completamento delle tutele previste dalla regolamentazione proposta: cosicché alla prevenzione, alle limitazioni e alle opportunità delineate dalle misure proposte si possa aggiungere anche la possibilità di far emergere situazioni di fatto pregiudizievoli per i minori.

Riferimenti bibliografici

- B. AGOSTINELLI (2023), *Minori in rete: l'illusione del consenso e l'equivoco della privacy*, in "Familia", 2023, n. 3
- E. BELISARIO, F. RICCIULLI (2024), *In piazza contro i porno deepfake e le discriminazioni digitali – Legge Zero #44*, in "Legge Zero", 6 ottobre 2024
- F. BRAVO (2017), *Il consenso e le altre condizioni di liceità del trattamento dei dati personali*, in G. Finocchiaro (a cura di), "Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali", Zanichelli, 2017
- R. CARRANO (2011), *Lo stato giuridico di figlio e il nuovo statuto dei diritti e doveri*, in "Giustizia civile", 2011, n. 4
- C. COLAPIETRO, A. IANNUZZI (2017), *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in C. Colapietro, L. Califano (a cura di), "Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679", Editoriale Scientifica, 2017
- V. CORRIERO (2004), *Privacy del minore e potestà dei genitori*, in "Rassegna di diritto civile", 2004, n. 4
- C. DI COSTANZO (2023), *La tutela costituzionale del minore: identità, salute e relazioni*, Giappichelli, 2023
- E. DOCKTERMAN (2013), *Should Parents Post Pictures of Their Kids on Facebook?*, in "Time", 6 September 2013
- G.P. DOLSO (2019), *Dignità, eguaglianza e Costituzione*, Edizioni Università di Trieste, 2019
- EUROPEAN DATA PROTECTION BOARD (2020), *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, 4 maggio 2020
- GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (2021), *Minori e nuove tecnologie - Consigli ai «Grandi» per un utilizzo sicuro da parte dei «Piccoli»*, febbraio 2021
- GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (s.d.), *Sharenting - Suggerimenti ai genitori per limitare la diffusione online di contenuti che riguardano i propri figli* - Pagina informativa
- W. GRISWOLD (2012), *Cultures and societies in a changing world*, SAGE Publications, 2012
- M. HERVIEU (2024), *Point sur la loi n° 2024-120 du 19 février 2024 visant à garantir le respect du droit à l'image des enfants*, Dalloz Actu Étudiant, 14 mars 2024
- K. KINDELAN (2024), *Ruby Franke's daughter speaks out to lawmakers on family vlogging dangers*, in "abcNews", 17 October 2024
- S. LECKART (2012), *The Facebook-Free Baby*, in "The Wall Street Journal", 15 May 2012

- L.M. LUCARELLI TONINI (2024), *Strumenti di age verification alla luce del contributo del Garante privacy e dell'AGCOM: il rischio di obsolescenza tecnologica e conoscitiva*, in "Rivista italiana di informatica e diritto", 2024, n. 2
- N. MEAKIN (2013), *The pros and cons of 'sharenting'*, in "The Guardian", 17 May 2013
- A.C. MORO (2014), *Manuale di diritto minorile*, Zanichelli, 2014
- M. OROFINO (2022), *La normativa a tutela dei minori nel Testo Unico per la fornitura di servizi di media audiovisivi con uno sguardo rivolto al regolamento (UE) 2022/2065*, in "MediaLaws", 2022, n. 3
- M. OROFINO (2018), *Minori e diritto alla protezione dei dati personali*, in M. Orofino, F. Pizzetti (a cura di), "Privacy, minori, cyberbullismo", Giappichelli, 2018
- S. PAGNI (2014), *La rappresentazione della donna nel cinema italiano del secondo dopoguerra: il caso di "Bellissima" di Luchino Visconti nei documenti d'archivio*, in "MA - Il mondo degli archivi", gennaio 2014
- F. RESTA (2022), *Sub art. 8 GDPR*, in G.M. Riccio, G. Scorza, E. Belisario (a cura di), "GDPR e normativa privacy. Commentario", Ipsoa, 2022



DOMIZIANO PIERANTONI

Minori su Internet: profili di responsabilità

Premessi alcuni cenni sul principio del *best interest of the child*, il saggio intende soffermarsi sul tema riguardante l'utilizzo di Internet da parte dei minori. In particolare, messa in luce l'esigenza di bilanciare adeguatamente, da un lato, i diritti di informazione e comunicazione, e, dall'altro lato, il diritto ad essere protetti dai rischi che ne minacciano uno sviluppo sano, ci si soffermerà sui profili di responsabilità che possono riguardare l'attività digitale dei più giovani. Da ultimo, si vuole sottolineare l'importanza di un'adeguata azione preventiva volta a incrementare nei genitori, cui è affidato il delicato compito di accompagnare i figli nell'utilizzo della rete, quelle specifiche competenze tecniche necessarie per assolvere al meglio ai loro doveri di educazione e vigilanza. Appare fondamentale, a tal fine, offrire un'opportuna "educazione civica al digitale" che, tra le altre cose, renda edotti gli utenti del web, secondo codici semiotici e modelli comunicativi adeguati alle differenti fasce di età, circa i profili di responsabilità cui possono andare incontro a fronte di un utilizzo "sconsiderato" dello stesso.

The best interest of the child – Minori su Internet – Responsabilità – Educazione civica al digitale

Children on the Internet: profiles of responsibility

Following an examination of the principle of the best interest of the child, this essay addresses the issue of Internet usage among minors. It particularly emphasizes the necessity of appropriately balancing, on one hand, the rights to information and communication, and on the other, the right to protection from risks that may jeopardize healthy development. The analysis will explore the aspects of responsibility associated with the digital activities of young individuals. Furthermore, the paper underscores the importance of implementing effective preventive measures aimed at equipping parents – who bear the crucial responsibility of guiding their children in Internet use – with the specific technical competencies required to fulfill their educational and supervisory duties. In this context, it is essential to provide an appropriate "digital civic education" that, among other objectives, informs web users – through semiotic codes and communication models tailored to various age groups – about the responsibilities they may encounter as a result of "reckless" Internet usage.

The best interest of the child – Children on the Internet – Responsibility – Digital civic education

L'Autore è dottorando di ricerca in Discipline giuridiche presso l'Università degli Studi Roma Tre

Questo contributo fa parte della sezione monografica *Minori e Internet* a cura di Carlo Colapietro e Antonio Iannuzzi

SOMMARIO: 1. Introduzione. – 2. *The best interest of the child* quale principio-cardine della tutela dei minori. – 3. Minori su Internet. – 4. Profili di responsabilità. – 5. La disciplina sul cyberbullismo. – 6. L'importanza di impartire un'adeguata educazione civica al digitale.

1. Introduzione

È molto dibattuto il tema riguardante l'utilizzo di Internet da parte dei minori. Come noto, si tratta di uno "spazio digitale" pensato e creato più a misura di adulto che di bambino, che, proprio in quanto tale, può risultare pregiudizievole per lo sviluppo sano del fanciullo.

Se è vero che il Web risulta senz'altro uno strumento particolarmente utile – al giorno d'oggi forse addirittura indispensabile – al fine di esercitare efficacemente il proprio diritto ad essere informati, informare e, più in generale, a comunicare ed esprimersi, è altrettanto vero che lo stesso può, soprattutto laddove a navigarvi sia un soggetto che non ha ancora sviluppato una piena maturità psichica, risultare assolutamente insidioso. Vicende giudiziarie e tristi accadimenti di cronaca ci forniscono, ahimè, uno spaccato piuttosto chiaro delle potenzialità (anche) negative insite nell'ampia diffusione degli strumenti digitali.

Alla base delle preoccupazioni destate dall'utilizzo di Internet da parte dei minori, v'è senza dubbio un'idea di profondo rispetto dell'infanzia, da intendersi non solo quale momento fondamentale di sviluppo dell'essere umano, bensì come realtà

già presente e meritevole di approfondita considerazione e tutela da parte degli "adulti".

Trasposte sul piano giuridico, tali considerazioni sollecitano una ricostruzione del modo in cui il diritto si incarica di rispondere all'esigenza di apprestare appropriate garanzie per la salvaguardia del minore in contesti evidentemente delicati come quello della rete.

Emerge, peraltro, la necessità di fornire un'adeguata "educazione civica al digitale" attraverso la quale, rivolgendosi ai genitori oltre che ai minori stessi, sia data la possibilità di istruire gli utenti del Web ad una corretta navigazione, consentendo di sviluppare una piena consapevolezza circa i profili di responsabilità che un uso sconsiderato dello stesso può far maturare.

Ciò, risulta ancor più urgente se si considera che al giorno d'oggi l'ambiente digitale sta diventando sempre più rilevante per molteplici aspetti della vita del minore: basti pensare ad alcuni dei tratti connotanti la recente esperienza pandemica causata dalla diffusione del c.d. Covid-19, durante la quale i servizi di comunità – inclusi l'istruzione, i servizi governativi e il commercio – hanno fatto ampio affidamento sulle tecnologie digitali¹.

1. L'importante incremento dell'impiego di Internet da parte dei minori verificatosi durante il periodo pandemico causato dal diffondersi del Covid-19 e dalle restrizioni necessarie al suo contenimento imposte dagli Stati ha suscitato attenzione sia nelle istituzioni europee (si vedano, ad esempio, la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Strategia dell'Ue per una lotta più efficace contro gli abusi sessuali su minori* COM (2020) 607, adottata il 24 luglio 2020; la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Strategia dell'Ue sui diritti dei minori (2021-2024)* COM(2021) 142, adottata il 24 marzo 2021); sia nel Comitato delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza, che, durante la sua 86ª Sessione (18 gennaio – 5 febbraio 2021) ha adottato il Commento generale n. 25 "Sui diritti dei minorenni in relazione all'ambiente digitale". Il Comitato, composto da diciotto esperti indipendenti, pubblica

Le innovazioni tecnologiche, dunque, di fatto finiscono per condizionare la vita dei minorenni e i loro diritti in modo ampio e interdipendente, anche laddove essi non abbiano accesso a Internet. L'inclusione digitale e, in seconda battuta, un accesso consapevole alla rete – oltre a combattere le disuguaglianze già esistenti e ad evitare che ne possano nascere di nuove – possono aiutarli a esercitare l'intera gamma dei propri diritti civili, politici, culturali, economici e sociali senza incorrere nei rischi che il mondo virtuale riserva.

2. The best interest of the child quale principio-cardine della tutela dei minori

Introdotte le tematiche che questo scritto intende affrontare, ci si soffermerà sul c.d. *best interest of the child*², che – assunto a principio fondamentale dalla Convenzione sui diritti del fanciullo dell'ONU³ – di fatto svolge il ruolo di colonna portante sulla quale poggia la regolazione di tutte le fattispecie legate all'infanzia⁴.

A partire dall'art. 3, co. 1, della Convenzione – in forza del quale «In tutte le decisioni relative ai fanciulli di competenza sia delle istituzioni pubbliche o private di assistenza sociale, dei tribunali, delle autorità amministrative o degli organi legislativi,

l'interesse superiore del fanciullo deve essere considerato preminente» – si è diffusa quell'impostazione che, rompendo con il passato, guarda al minore non più come oggetto di diritti e di pretese altrui, bensì quale soggetto titolare di diritti propri, tutelati e protetti dall'ordinamento⁵.

Impostazione, questa, che è penetrata negli ordinamenti sovranazionale e nazionali grazie al larghissimo consenso di cui ha goduto la Convenzione, nonché all'interpretazione ad essa «orientata» che è stata data ai riferimenti ai diritti dei minori contenuti nelle Carte costituzionali.

Quanto a ciò che ci interessa più da vicino, è dato riscontrare come il diritto eurounitario non sia risultato impermeabile alla diffusione del principio *de quo*: esso, infatti, oltre a trovare esplicita collocazione nella Carta dei diritti fondamentali dell'Unione europea – il cui art. 24, co. 2, stabilisce che «In tutti gli atti relativi ai bambini, siano essi compiuti da autorità pubbliche o da istituzioni private, l'interesse superiore del bambino deve essere considerato preminente» – è entrato a far parte dello strumentario ermeneutico a disposizione della Corte di Giustizia europea, dalla cui giurisprudenza emerge chiaramente la consapevolezza del ruolo dirimente svolto dal diritto

regolarmente la propria interpretazione del contenuto delle norme sui diritti umani, nella forma di Commenti generali su questioni tematiche, al fine di assistere gli Stati parte nel compimento degli obblighi che derivano loro dall'aver ratificato la Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza. Il documento in questione, in particolar modo, è stato redatto all'esito di una consultazione svolta con la partecipazione di oltre 700 tra ragazzi e ragazze di età compresa tra i 9 e i 22 anni, provenienti da 27 Stati parte, cui è stato chiesto quale impatto abbia avuto la tecnologia digitale sui loro diritti e quali debbano essere, a loro avviso, le azioni da intraprendere per proteggerli.

2. Per un'ampia panoramica sul superiore interesse del minore, cfr. BIANCA 2021.
3. La Convenzione sui diritti del fanciullo è stata approvata dall'Assemblea generale delle Nazioni Unite a New York il 20 novembre 1989 e ratificata dall'Italia con legge 27 maggio 1991, n. 176. La Convenzione ha avuto un larghissimo seguito nell'ambito della comunità internazionale, tanto da aver ricevuto più di 190 ratifiche. È stata poi integrata con tre Protocolli opzionali tutti eseguiti e in vigore per l'Italia: il primo riguardante la vendita delle persone di minore età, la prostituzione infantile e la pornografia rappresentante i minori (*Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography* – OPSC); il secondo relativo al coinvolgimento dei minori nei conflitti armati (*Optional Protocol on Children in Armed Conflict* – OPAC); il terzo sulle procedure di reclamo (*Optional Protocol to the Convention on the Rights of the Child on a communications procedure*). In generale, sulla Convenzione si veda, tra gli altri, AUTORITÀ GARANTE PER L'INFANZIA E L'ADOLESCENZA 2019.
4. Adottando una prospettiva diacronica, la Convenzione di New York del 1989 sembra aver segnato un momento di svolta fondamentale anche per quel che riguarda la declinazione domestica dei diritti relativi ai minori. Sul punto v. PITTO 2023, p. 42 ss.
5. *Ivi*, p. 37; FERRANDO 1998.

internazionale in materia. Nell'ottica del giudice lussemburghese, che in più occasioni ha fatto riferimento al principio del *the best interest of the child* quale fondamentale canone interpretativo per quel che concerne le fattispecie relative ai minori, la Convenzione di New York del 1989 rappresenta il punto di riferimento nella valutazione della conformità del diritto dell'Unione con gli standard internazionali in tema di diritti dei minori⁶.

Un ruolo di precipua importanza in questo processo è stato senz'altro svolto anche dalla Corte europea dei diritti dell'uomo, la quale – accogliendo nel proprio ragionamento le norme della Convenzione di New York del 1989 e muovendo i passi dai riferimenti (impliciti) presenti nel testo di cui è custode⁷ – è arrivata anch'essa ad attribuire al principio in questione un'importanza cruciale ogniquale si tratti di operare un bilanciamento concreto tra l'interesse del minore e quelli dei genitori e/o degli altri parenti del fanciullo⁸.

Volgendo lo sguardo al nostro contesto domestico, è dato riscontrare come il disegno costituzionale in materia di minori, lungi dall'esaurirsi nelle previsioni di cui agli art. 30 e 31 Cost., si completa alla luce dei principi ispiratori dell'intera Carta, quali, in particolare, il principio personalista di cui all'art. 2 – in forza del quale è dato porre la persona al centro non solo dell'ordinamento generale, ma dello stesso ordinamento familiare – e il principio generale di eguaglianza di cui all'art. 3⁹.

Più nel dettaglio, una lettura sistematica della nostra Carta fondamentale consente di rilevare come nella prospettiva del modello di società e di famiglia prefigurato dagli artt. 2, 3 e 29 Cost., le norme costituzionali che interessano la posizione istituzionale del minore contenute negli artt. 30 e 31 Cost., oltre a respingere gli antiquati (ma fino ad allora tradizionali) modelli di autoritarismo educativo, integrano un autentico statuto dei diritti dell'infanzia e della gioventù. Esse impegnano

6. Cfr. Corte di Giustizia UE, sent. 27 giugno 2006, causa C-540/03. In dottrina, (MAGLI-SPADARO 2020, p. 9 ss.) è stato rilevato come la Corte di Giustizia si sia mostrata forse più timida nell'interpretazione del principio limitandolo ai più stretti margini stabiliti dall'art. 24 della Carta di Nizza. Ciò, a fronte della diversa tendenza della Corte EDU, secondo cui l'interesse del minore deve assumere valore fondamentale in tutte le decisioni relative a minori. Sul punto, v. Corte europea dei diritti dell'uomo, *Neulinger e Shuruk c. Svizzera*, 6 luglio 2010.

7. In effetti, la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali non presenta, almeno formalmente, l'aspetto di un trattato *child-friendly*: le sue potenzialità per la tutela dei diritti dei minori non sono, pertanto, a prima vista evidenti. Essa menziona espressamente i minori unicamente nei suoi articoli 5 e 6, oltreché nell'art. 2 del I Protocollo addizionale, e non contiene nessuno specifico riferimento al principio del superiore interesse del minore, le cui origini, d'altronde, sono cronologicamente successive. Nello specifico, l'art. 5 della CEDU sancisce un'eccezione al diritto alla libertà personale dei minori, prevedendo i casi in cui essi possono essere legittimamente privati della loro libertà. L'art. 6, dedicato al diritto ad un equo processo, stabilisce che l'accesso all'aula d'udienza può essere vietato alla stampa e al pubblico, durante tutto o parte del procedimento, quando lo esigono gli interessi del minore. L'art. 2 del I Protocollo addizionale stabilisce che il diritto all'istruzione non può essere rifiutato a nessuno e contempla l'obbligo per lo Stato di rispettare il diritto dei genitori di provvedere all'educazione e all'insegnamento dei figli secondo le loro convinzioni religiose e filosofiche. La giurisprudenza della Corte europea dei diritti dell'uomo, però, fa frequente riferimento a trattati che interessano, a vario titolo, le persone di minore età, ed è soprattutto alla Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza che guarda quando è chiamata ad applicare le disposizioni della CEDU in contesti in cui vengono in gioco diritti di persone di minore età. La Convenzione di New York, del resto, è stata ratificata da quasi tutti gli Stati del mondo – ivi inclusi tutti gli Stati parte della CEDU – e alcune delle regole in essa contenute sono ormai ritenute corrispondenti al diritto internazionale consuetudinario. Tra questi, il principio del superiore interesse del minore, cui la giurisprudenza della Corte europea assegna un ruolo centrale. I casi in cui esso viene perlopiù in rilievo riguardano ricorsi relativi alla lamentata violazione dell'art. 8 della CEDU, che sancisce il diritto alla vita privata e familiare.

8. Così a partire dalla sentenza 7 agosto 1996, *Johansen*. Cfr. in seguito, fra le altre sentenze, 9 giugno 1998, *Bronda*; 13 luglio 2000, *Elsholz*; 13 luglio 2000, *Scozzari e Giunta*; 11 ottobre 2001 *Hoffmann*; 11 ottobre 2001, *Sahin*; 11 ottobre 2001, *Sommerfeld*; 16 luglio 2002, P., C., e S.; 5 dicembre 2002, *Hoppe*.

9. Cfr. LAMARQUE 2006, p. 629.

a considerare le singole disposizioni in tema non quali forme episodiche di tutela di soggetti istituzionalmente deboli, ma come elementi costitutivi di una strategia di intervento legislativo dove il concetto del *favor minoris* assume la portata di vera e propria promozione dei diritti del minore individuato nella sua condizione di cittadino *in fieri*¹⁰.

Quanto alla formazione dei minori – che, come vedremo, oggi deve necessariamente riguardare anche il mondo del digitale – la Costituzione, lungi dal separare i problemi legati alla condizione minorile dai temi generali della trasformazione della società, delinea un complessivo diritto all'educazione che non investe solo lo *status* familiare dei singoli, ma riguarda più in generale la loro posizione nell'universo sociale.

Risulta significativo, peraltro, il fatto che i Padri costituenti abbiano scelto di investire lo Stato del ruolo di garante dell'effettività dei diritti del fanciullo. Aspetto, questo, che emerge chiaramente dall'art. 30, co. 2, Cost., in forza del quale il legislatore è incaricato di provvedere a che siano assolti i compiti dei genitori laddove questi risultino impossibilitati a svolgere il loro primario diritto-dovere al mantenimento, all'istruzione e all'educazione dei figli¹¹.

In questa prospettiva di integrazione tra l'aspetto privato e la dimensione pubblica dei problemi della condizione minorile, il diritto all'educazione concreta aspettative costituzionalmente protette, impegnando la Repubblica agli adempimenti richiesti per assicurare al minore tutti gli strumenti

necessari per partecipare pienamente, consapevolmente e, soprattutto, senza rischi all'organizzazione politica, economica e sociale del Paese.

Il sistema si è poi ulteriormente evoluto grazie al ruolo determinante della Corte costituzionale¹², la quale, sulla base delle disposizioni contenute nella nostra Legge fondamentale, ha progressivamente affermato la presenza nell'ordinamento costituzionale di un *favor minoris* su cui il legislatore è chiamato a fondare l'intero sistema delle relazioni familiari¹³, improntando la relativa disciplina verso l'individuazione di una tutela "specializzata" per il fanciullo¹⁴.

In altri termini, il Giudice delle leggi ha evidenziato la necessità costituzionale che il legislatore e l'interprete, ciascuno nel proprio ambito, operino un bilanciamento tale per cui in ogni rapporto giuridico sostanziale o processuale nel quale risulti coinvolto un minore, il suo interesse concreto prevalga sempre su quello di ogni altro soggetto¹⁵. Il tutto, peraltro, guardando al figlio come ad una persona titolare di diritti propri e ai genitori come responsabili di una vera e propria funzione di matrice costituzionale finalizzata alla formazione personale del primo.

A ben vedere, il principio in questione finisce per assumere un "duplice volto", costituendo ad un tempo un obiettivo – che impone agli Stati di tenere in considerazioni gli interessi plurimi del minore in ogni processo decisionale che lo riguardi, pubblico o privato che sia – e uno strumento interpretativo alla luce del quale leggere le concrete

10. Cfr. BESSONE 1976, p. 86 ss.

11. Art. 30 Costituzione: «È dovere e diritto dei genitori mantenere, istruire ed educare i figli, anche se nati fuori del matrimonio. Nei casi di incapacità dei genitori, la legge provvede a che siano assolti i loro compiti. La legge assicura ai figli nati fuori del matrimonio ogni tutela giuridica e sociale, compatibile con i diritti dei membri della famiglia legittima. La legge detta le norme e i limiti per la ricerca della paternità».

12. Cfr., da ultimo, Corte cost. sent. 23 aprile 2024, n. 71, che, nel dichiarare non fondata la questione di legittimità costituzionale dell'art. 574-bis c.p. sollevata, con riferimento all'art. 3 Cost., dal Tribunale ordinario di Cuneo, ribadisce come la responsabilità genitoriale vada esercitata nell'interesse dei minori.

13. Cfr. in particolare Corte cost. sent. 10 febbraio 1981, n. 11. La Corte in tale sentenza analizza il riferimento all'interesse del minore di cui alla legge 5 giugno 1967, n. 431, affermando che tale complesso normativo considera la tutela dell'interesse del minore infraotenne in stato di abbandono in posizione di preminenza rispetto a tutti gli altri, compresi quelli dei genitori naturali. La stessa Consulta nella decisione ammette l'esistenza in tale disciplina di «tratti decisamente innovatori».

14. Cfr. FERRANDO 1998, p. 168.

15. Cfr. LAMARQUE 2006, p. 630.

fattispecie e bilanciare il ruolo degli adulti rispetto ai minori d'età¹⁶.

La clausola generale del *the best interest of the child*, in altri termini, costituisce lo strumento per dare attuazione, nella varietà delle situazioni concrete, ai preminenti diritti del minore, orientando alla sua realizzazione le decisioni che lo riguardano.

In tal maniera, emerge un *best interest* dai connotati particolarmente flessibili e dinamici, che richiede una valutazione misurata al contesto specifico, essendo in grado sia di adeguarsi alla dimensione individuale, tenendo conto delle specifiche condizioni in cui versa il minore, soprattutto laddove ricorrano situazioni di particolare fragilità; sia di tenere il passo con e, anzi, stimolare l'evoluzione del sistema, nel senso di un progressivo sviluppo delle risposte fornite alle esigenze cui, nell'ambito di una società sempre più complessa e articolata, i minori vanno incontro¹⁷.

3. Minori su Internet

È notorio il fatto che l'utilizzo di Internet – soprattutto laddove declinato nell'utilizzo dei cc.dd. *social media networks* – sia ormai diffusissimo non solo tra i giovani, bensì anche tra i giovanissimi.

Nonostante il c.d. “nuovo” Codice della privacy¹⁸ all'art. 2-*quinquies*, rubricato «Consenso del minore in relazione ai servizi della società

dell'informazione», stabilisca che solo a partire dai quattordici anni il minore può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione di turno, sempre più spesso sui social è dato rinvenire la presenza di account di minori di quattordici anni, i quali non solo partecipano attivamente alla vita digitale delle piattaforme, ma spesso e volentieri attraverso le stesse svolgono attività remunerativa. Si pensi, a tal proposito, al fenomeno dei cc.dd. *baby influencers*, che prestando la loro immagine, sponsorizzano attraverso i propri canali social servizi e prodotti di qualunque genere.

Ora, è chiaro che l'utilizzo di Internet e dei social da parte dei minori risponde anche all'esigenza di esercitare adeguatamente, ovvero sia al passo con la spiccata “digitalizzazione” della realtà che contraddistingue l'epoca attuale, il diritto all'informazione e alla comunicazione.

Diritto, questo, che, espressamente tutelato sia in fonti sovranazionali¹⁹ sia nella Costituzione repubblicana del '48 – la quale all'art. 21, co. 1, espressamente stabilisce che «tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione» – deve oggi declinarsi tenendo conto dell'utilizzo diffuso della rete e dei dispositivi che consentono di accedere ad essa²⁰.

16. Cfr. DI NAPOLI 2023, p. 69.

17. *Ibidem*.

18. “Nuovo” alla luce delle modifiche apportate dal d.lgs. 10 agosto 2018, n. 101, il quale ha adeguato la normativa nazionale in materia di trattamento e di tutela dei dati personali alle novità apportate dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio.

19. Ci si riferisce: alla Convenzione europea dei Diritti dell'Uomo, firmata a Roma il 4 novembre del 1950, che al paragrafo 1 dell'art. 10, rubricato “Libertà di espressione”, prevede che: «Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. Il presente articolo non impedisce agli Stati di sottoporre a un regime di autorizzazione le imprese di radiodiffusione, cinematografiche o televisive»; alla Carta dei diritti fondamentali dell'Unione europea del 2000, che, al paragrafo 1 dell'art. 11, rubricato «Libertà di espressione e d'informazione», sancisce che: «Ogni individuo ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera».

20. A tal proposito è interessante osservare il riferimento che l'art. 17 della Convenzione di New York fa ai mass media, sancendo il diritto all'informazione delle persone di minore età: dal 1989, l'avvento di Internet e lo sviluppo dell'ambiente digitale come luogo di opportunità ma anche di potenziali pericoli ha certamente inciso sull'applicazione della Convenzione, promuovendone un cambio di prospettiva e un'attualizzazione dei contesti entro cui i diritti possono svilupparsi. Di seguito il testo del citato art. 17: «Gli Stati parti riconoscono l'importanza della

Peraltro, come si diceva anche in apertura, la pandemia da Covid-19 e le restrizioni necessarie al suo contenimento imposte dagli Stati hanno portato a un importante incremento dell'impiego di Internet, soprattutto da parte delle persone di minore età.

D'altro canto, indubbiamente la rete presenta, al fianco di potenzialità senz'altro positive, anche degli aspetti particolarmente insidiosi, che inevitabilmente si acquisiscono quando a navigare sono soggetti minori d'età, rispetto ai quali, proprio per questo, è necessario prestare particolare attenzione perché potrebbero, più di altri, risultare inconsapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate, nonché dei diritti che gli spettano²¹.

Ebbene, anche per quel che concerne il tema della presenza dei minori sul web, il *best interest of the child*, è chiamato a svolgere il ruolo di principio-cardine. Ciò emerge chiaramente dalla *Strategia del Consiglio d'Europa per i diritti delle persone di minore età* per il quinquennio 2022-2027: si tratta di uno strumento di indirizzo a carattere non vincolante, centrale nel panorama della tutela e della promozione dei diritti delle persone di minore età a livello europeo, che si pone l'obiettivo di sviluppare una visione condivisa e degli obiettivi comuni per tutelare e valorizzare i diritti dei minori²².

Il documento, in particolar modo, indica sei obiettivi prioritari che il Consiglio d'Europa si impegna a promuovere nel periodo di riferimento²³. Tra questi, due risultano qui di particolare interesse: la prima priorità punta ad assicurare ai bambini una vita libera da violenze, fisiche o psicologiche, compresi l'abuso e lo sfruttamento sessuale, nonché gli atti di bullismo, anche praticati attraverso i social media. Il quarto obiettivo prioritario riguarda la vita delle persone di minore età nell'ambiente digitale e punta a garantire che i giovani godano delle opportunità di conoscenza e di dialogo offerte dalla rete e dai social media senza incorrere nei potenziali pericoli cui le nuove tecnologie li espongono.

È evidente, dunque, il delicato punto di equilibrio che si è chiamati a individuare: consentire ai minori di accedere alla rete al fine di esercitare i propri diritti costituzionalmente rilevanti, allo stesso tempo prestando adeguata attenzione perché la stessa non si riveli un'arma a doppio taglio in grado di ledere o minacciare il loro sviluppo e la loro formazione.

A tal proposito, i genitori – cui, come detto, la Costituzione attribuisce il diritto-dovere di «mantenere, istruire ed educare i figli, anche se nati fuori del matrimonio» – assumono un ruolo di fondamentale importanza. Una lettura dell'art. 30 Cost.

funzione esercitata dai mass media e vigilano affinché il fanciullo possa accedere a una informazione e a materiali provenienti da fonti nazionali e internazionali varie, soprattutto se finalizzati a promuovere il suo benessere sociale, spirituale e morale nonché la sua salute fisica e mentale. A tal fine, gli Stati parti: Incoraggiano i mass media a divulgare informazioni e materiali che hanno una utilità sociale e culturale per il fanciullo e corrispondono allo spirito dell'art. 29; Incoraggiano la cooperazione internazionale in vista di produrre, di scambiare e di divulgare informazioni e materiali di questo tipo provenienti da varie fonti culturali, nazionali e internazionali; Incoraggiano la produzione e la diffusione di libri per l'infanzia; Incoraggiano i mass media a tenere conto in particolar modo delle esigenze linguistiche dei fanciulli autoctoni o appartenenti a un gruppo minoritario; Favoriscono l'elaborazione di principi direttivi appropriati destinati a proteggere il fanciullo dalle informazioni e dai materiali che nuocciono al suo benessere in considerazione delle disposizioni degli artt. 13 e 18».

21. La giurisprudenza ha evidenziato come tale esigenza di tutela trovi fondamento nell'art. 16 della Convenzione di New York del 1989, che sancisce il diritto di ogni minore a non subire interferenze arbitrarie o illegali con riferimento alla vita privata, alla propria corrispondenza o al domicilio, oltreché il diritto a non subire lesioni alla reputazione e all'onore. In tal senso, cfr. Tribunale per i minorenni di Caltanissetta, 16 luglio 2018.
22. *Council of Europe Strategy for the Rights of the Child (2022-2027)*. La Strategia è frutto di un ampio confronto tra Stati membri, organizzazioni internazionali, organizzazioni della società civile e 220 minorenni provenienti da tutta Europa.
23. Più nello specifico, la *Strategia* per il quinquennio 2022-2027 si pone i seguenti obiettivi: 1. Proteggere i minorenni dalla violenza; 2. Assicurarsi che tutti i minori abbiano pari opportunità e siano inclusi nella società; 3. Favorire l'accesso dei minori ai dispositivi tecnologici e al loro uso sicuro; 4. Rendere l'accesso alla giustizia più facile ai minorenni; 5. Dar voce a ciascun minore; 6. Sostenere i minori in situazioni di crisi e di emergenza.

alla luce degli artt. 2 e 3 della stessa Carta suggerisce che il *dovere* di cui sopra implichi una generale cura della persona del minore. Quanto, invece, al *diritto* dei genitori, esso, lungi dal poter essere inteso come loro libertà personale, si traduce in funzione educativa da svolgersi nei confronti e nell'esclusivo interesse dei figli, nel rispetto delle libertà che la Costituzione garantisce anche ai minori (artt. 8, 13, 14, 21, 49 ecc), affinché ad essi sia assicurato uno sviluppo sano e integrale della personalità²⁴.

Funzione educativa, questa, che deve necessariamente riguardare anche l'utilizzo della rete²⁵. La giurisprudenza, in effetti, è chiara nell'affermare che ai genitori compete un compito educativo e, di fianco ad esso, un compito di vigilanza circa le concrete modalità operative che contraddistinguono la presenza dei minori sul Web.

Più nello specifico, riguardo all'uso della rete telematica l'adempimento del dovere di vigilanza dei genitori è strettamente connesso all'estrema pericolosità di quel sistema e alla relativa potenziale incontrollabile esondazione dei contenuti immessi in circolo²⁶.

In altri termini, i genitori, in virtù del loro ufficio, ossia dei compiti che la legge impone per

assicurare la tutela dei figli, sono chiamati a educarli all'utilizzo degli strumenti che l'evoluzione tecnologica offre e di vigilare sul loro operato affinché sui loro dispositivi elettronici non compaiano materiali non adatti alla loro età e formazione educativa, nonché al fine di preservarli dal danno che essi possono arrecare agli altri e a sé stessi²⁷.

4. Profili di responsabilità

Volgendo l'attenzione ai profili di responsabilità che, direttamente o indirettamente, possono riguardare l'attività svolta dai minori o dai genitori degli stessi sul Web, è dato anzitutto considerare il caso in cui il comportamento del minore integri una delle fattispecie di reato previste dal nostro ordinamento. Come noto, l'art. 27, co. 1, della Costituzione stabilisce che «La responsabilità penale è personale», cosicché deve escludersi che i genitori possano essere chiamati a rispondere penalmente per un fatto altrui.

Ad essere perseguito sarà, invece, il minore stesso, laddove maggiore di quattordici anni. In caso contrario, troverà applicazione l'art. 97 c.p., in forza del quale è sempre esclusa l'imputabilità dell'infraquattordicenne. Quest'ultimo, in altri termini, anche laddove autore di un fatto di reato, non potrà

24. Cfr. la relazione illustrativa al d.lgs. 28 dicembre 2013, n. 154 (*Revisione delle disposizioni vigenti in materia di filiazione, a norma dell'articolo 2 della legge 10 dicembre 2012, n. 219*), ove – con riferimento alla nozione di responsabilità genitoriale, introdotta superando quella di potestà genitoriale – si sottolinea come i contenuti dell'impegno genitoriale sono da considerarsi alla stregua di un'assunzione di responsabilità da parte del genitore nei confronti dei figli: «La modifica terminologica dà risalto alla diversa visione prospettica che nel corso degli anni si è sviluppata ed è ormai da considerare patrimonio condiviso: i rapporti genitori-figli non devono essere più considerati avendo riguardo al punto di vista dei genitori, ma occorre porre in risalto il superiore interesse dei figli minori». A tal proposito, v. anche Corte cost., 29 maggio 2020, n. 102.

25. Cfr. RAVERA 2019.

26. Cfr. Tribunale per i minorenni di Caltanissetta, 8 ottobre 2019, secondo cui: «è bene porre in evidenza che gli obblighi inerenti la responsabilità genitoriale impongono non solo il dovere di impartire al minore una adeguata educazione all'utilizzo dei mezzi di comunicazione ma anche di compiere un'attività di vigilanza sul minore per quanto concerne il suddetto utilizzo; l'educazione si pone, infatti, in funzione strumentale rispetto alla tutela dei minori al fine di prevenire che questi ultimi siano vittime dell'abuso di internet da parte di terzi. L'educazione deve essere, inoltre, finalizzata a evitare che i minori cagionino danni a terzi o a sé stessi mediante gli strumenti di comunicazione telematica; sotto tale profilo si deve osservare che l'anomalo utilizzo da parte del minore dei mezzi offerti dalla moderna tecnologia tale da ledere la dignità cagionando un serio pericolo per il sano sviluppo psicofisico dello stesso, può essere sintomatico di una scarsa educazione e vigilanza da parte dei genitori; i genitori sono tenuti non solo ad impartire ai propri figli un'educazione consona alle proprie condizioni socio-economiche, ma anche ad adempiere a quell'attività di verifica e controllo sulla effettiva acquisizione di quei valori da parte del minore».

27. Cfr., a tal proposito, Tribunale civile di Parma, sez. I, 5 agosto 2020, n. 698.

essere destinatario di un rimprovero personale²⁸. Perché ciò accada, infatti, è necessario che il reo, al momento della commissione della condotta, fosse capace di intendere e di volere; capace cioè, da un lato, di comprendere il significato sociale e le conseguenze dei propri atti, nonché, dall'altro lato, di autodeterminarsi liberamente. Solo in presenza di tali condizioni, che il legislatore presume in via assoluta non sussistenti quando il reato sia commesso da un infraquattordicenne, la minaccia della pena potrà effettivamente indurre il soggetto ad astenersi da questo o quel comportamento. Solo in presenza di tali condizioni, dunque, la condotta *contra legem* assumerà effettivamente un livello di disvalore tale da giustificare l'irrogazione della pena.

Quanto, invece, ai cc.dd. "grandi minori", lungi dall'escluderne in via assoluta l'imputabilità, il legislatore considera il fatto che le capacità intellettuali e i poteri di inibizione si formano gradualmente, attraverso un processo che si sviluppa secondo tempi che non sono eguali per tutti, senza che, peraltro, ci sia sempre sincronia tra maturazione intellettuale e volitiva. Così che, gli stessi saranno imputabili solo nell'ipotesi in cui, con riferimento al caso di specie, risultino in grado sia di intendere che di volere (ma, ai sensi dell'art. 98, co. 1, c.p., laddove la responsabilità venga effettivamente accertata in sede processuale, il minore potrà comunque beneficiare di una diminuzione di pena nella misura massima di un terzo).

Il giudice dovrà, dunque, verificare caso per caso se il minore avesse, al momento del fatto, raggiunto una maturità psichica tale da consentirgli di comprendere il disvalore sociale del proprio agire. Accertamento, questo, che va compiuto tenendo a mente le specificità del reato commesso, potendo l'agente presentare un grado sufficiente di maturità rispetto a certe condotte e difettarne invece rispetto ad altre, potendo cioè ricorrere l'ipotesi di un'imputabilità "settoriale", da affermarsi con riferimento ad alcune classi di fatti e da negarsi, invece, per altre.

Caso ulteriore è quello del minore ultraquattordicenne affetto da infermità parziale di mente: laddove essa abbia inficiato il normale sviluppo psichico del minore ritardando il suo processo di maturazione si applicherà l'art. 98 c.p.; se, invece, il vizio parziale di mente si è manifestato su un

soggetto già maturo a venire in rilievo sarà l'art. 89 c.p., in virtù del quale, a fronte di uno stato di mente tale da scemare grandemente, senza però escludere del tutto, la capacità di intendere e di volere, il reo si vedrà irrogata una pena diminuita. Opportuno sottolineare come laddove l'infermità di mente sia totale, cioè tale da escludere del tutto la capacità di comprendere il disvalore delle proprie azioni e/o di autodeterminarsi, in luogo dell'art. 89 c.p., troverà applicazione la disciplina prevista dall'art. 88 c.p., a mente del quale, ancora una volta, viene esclusa l'imputabilità del soggetto agente.

In altri termini, dunque, se con riferimento all'infraquattordicenne è esclusa in via assoluta la capacità di intendere e di volere, il legislatore presume, seppur in via solamente relativa, la maturità intellettuale e volitiva dei minori ultraquattordicenni.

Quanto al versante civilistico, invece, occorre considerare l'ipotesi in cui il fatto illecito commesso dal minore cagioni un danno ingiusto ad altri.

Ebbene, l'art. 147 c.c., come noto, nel disciplinare i doveri dei genitori nei confronti dei figli, pone in capo ad ambedue i coniugi l'obbligo di mantenere, istruire, educare e assistere moralmente i figli, nel rispetto delle loro capacità, inclinazioni naturali e aspirazioni.

Per quel che concerne l'utilizzo della rete, come già detto, la giurisprudenza è chiara nell'affermare che ai genitori compete un compito educativo e, di fianco ad esso, un compito di vigilanza circa le concrete modalità di navigazione da parte dei minori.

Se ne ricava che laddove il minore si renda autore di un fatto illecito commesso tramite Internet a risponderne civilmente possano essere gli esercenti la responsabilità genitoriale sullo stesso. A tal proposito, la disposizione di riferimento è l'art. 2048 c.c., in forza del quale «Il padre e la madre, o il tutore sono responsabili del danno cagionato dal fatto illecito dei figli minori non emancipati o delle persone soggette a tutela, che abitano con essi». Previsione normativa, questa, che va coordinata con quella che sancisce la responsabilità per il fatto dannoso degli incapaci (2047 c.c.), cosicché i genitori e i tutori rispondono dei fatti illeciti compiuti da persone capaci di intendere e di volere, mentre se l'autore del danno è un incapace d'intendere o di

28. «Il minore di anni quattordici, laddove ricorrano i presupposti previsti dalla legge, può essere sottoposto ad una misura di sicurezza» (art. 224 c.p.).

volere troverà applicazione la norma sulla responsabilità dei sorveglianti.

In particolare, nel primo caso la responsabilità trova fondamento in una presunzione *iuris tantum* di difetto di educazione e di vigilanza; nel secondo caso, invece, in una presunzione *iuris tantum* di difetto di sorveglianza. Le indicate ipotesi di responsabilità presunta, pertanto, si pongono su un piano non concorrente, ma alternativo, alla stregua dell'accertamento, nel caso concreto, della sussistenza o meno di quella capacità²⁹.

Si tratta di responsabilità per fatto altrui a titolo di colpa personale, e precisamente di colpa presunta. Questi soggetti, ovverosia i genitori e i tutori, possono andare esenti da responsabilità provando di non avere potuto impedire il fatto pur avendo opportunamente sorvegliato e, ancor prima, adeguatamente educato il minore al rispetto delle persone e dei beni altrui (art. 2048, comma 3, c.c.)³⁰. A tal proposito, la Suprema Corte ha chiarito come essi «per superare la presunzione di colpa prevista dall'art. 2048 c.c., debbono fornire non la prova legislativamente predeterminata di non aver potuto impedire il fatto (atteso che si tratta di prova negativa), ma quella positiva di aver impartito al figlio una buona educazione e di aver esercitato su di lui una vigilanza adeguata, il tutto in conformità alle condizioni sociali, familiari, all'età, al

carattere e all'indole del minore. L'inadeguatezza dell'educazione impartita e della vigilanza esercitata su un minore, fondamento della responsabilità dei genitori per il fatto illecito dal suddetto commesso, può essere desunta, in mancanza di prova contraria, dalle modalità dello stesso fatto illecito, che ben possono rivelare il grado di maturità e di educazione del minore, conseguenti al mancato adempimento dei doveri incombenti sui genitori, ai sensi dell'art. 147 c.c.»³¹.

Quanto all'attività di vigilanza – consistente nel controllare ed eventualmente vietare che il figlio intraprenda attività illecite o che per la loro pericolosità richiedono l'adozione di particolari misure di cautela, che, ad avviso della giurisprudenza, per quel che riguarda l'utilizzo degli strumenti digitali possono concretizzarsi in una limitazione quantitativa e qualitativa dell'accesso alla rete Internet da parte del minore³² – occorre evidenziare la necessità di bilanciare adeguatamente l'attività di controllo che il genitore è tenuto ad espletare con il diritto del minore alla riservatezza, cosicché ogni intromissione nella sfera privata del giovane dovrà essere giustificata dalle circostanze che connotano il caso di specie.

In effetti, il diritto-dovere di vigilare sulle comunicazioni del minore da parte del genitore non giustifica indiscriminatamente qualsiasi altrimenti

29. Cfr. BIANCA 2021-A, p. 662 ss.

30. Cfr. Tribunale civile di Sulmona, 9 aprile 2018, n. 103, che, in relazione ad un caso che vedeva dei soggetti minorenni autori della diffusione tramite social networks, senza il consenso dell'interessata, di fotografie contenenti l'immagine del nudo di una coetanea, riconosceva come civilmente responsabili, ex art. 2048, c. 1, c.c., i genitori degli autori della predetta diffusione, in quanto rimproverabili di *culpa in vigilando* ed *in educando*. In particolare, il giudice osservava come «non può non rilevarsi come la disposizione richiamata trasli in capo al genitore l'onere di provare e di dimostrare il corretto assolvimento dei propri obblighi educativi e di controllo sul figlio, solo in tal modo potendosi esonerare dalla condanna risarcitoria. Nella specie, nulla è stato dimostrato. Anzi, i fatti – quello della pubblicazione su Facebook, ma anche le singole cessioni, non autorizzate da V., dell'immagine a nudo di una coetanea – esprimono, di per sé, una carenza educativa degli allora minorenni, dimostratisi in tal modo privi del necessario senso critico, di una congrua capacità di discernimento e di orientamento consapevole delle proprie scelte nel rispetto e nella tutela altrui». Cfr. anche Tribunale civile di Teramo, 16 gennaio 2012, n. 18, secondo il quale: «Nel momento in cui i genitori, consapevoli delle potenzialità e dei rischi di internet, acconsentono ad un accesso del proprio figlio minore alla rete, quella doverosa attività di verifica e controllo a posteriori dell'indottrinamento educativo del proprio figlio, non può non fare i conti con l'estrema pericolosità di quel navigare in rete. E quella attività genitoriale di controllo appare tanto più doverosa in un periodo storico in cui sollecitazioni negative aggrediscono la sensibilità dei minori fin nei luoghi ritenuti più sicuri».

31. Corte Cass., sez. III civ., sent. n. 26200/2011.

32. Cfr. Tribunale civile di Parma, sez. I, 5 agosto 2020, n. 698; Tribunale per i minorenni di Caltanissetta, 8 ottobre 2019, cit.

illecita intrusione nella sfera di riservatezza del primo, ma solo quelle interferenze determinate da un'effettiva necessità, da valutare secondo le concrete circostanze del caso e, ad ogni modo, sempre nell'ottica della tutela del *best interest of the child*. È, d'altra parte, con riguardo a tale interesse che può apprezzarsi il disvalore della condotta del genitore, valutando se il pregiudizio determinato alla sfera personale del fanciullo giustifichi o meno vuoi la decadenza dalla responsabilità genitoriale (art. 330 c.c.), vuoi l'emissione dei provvedimenti giudiziali di cui all'art. 333 c.c.

Interessante è anche il caso in cui il minore sia "oggetto" di pubblicazione di materiale foto-video su Internet.

Ebbene, a tal proposito la giurisprudenza è chiara nell'affermare che la pubblicazione di contenuti o notizie ritraenti un minore sia atto eccedente l'ordinaria amministrazione. È evidente, infatti, come il caricamento online di foto o comunque di materiale riguardante soggetti minori costituisca un comportamento potenzialmente pregiudizievole per essi, in quanto determinante la diffusione delle immagini/informazioni fra un numero

indeterminato di persone, conosciute e non, tra le quali può celarsi qualche malintenzionato. Non può, ad esempio, andare sottaciuto il pericolo costituito dalla condotta di soggetti che, con procedimenti di fotomontaggio, utilizzino foto reperite sul Web per produrre del materiale pedopornografico da far circolare fra gli interessati³³.

In quanto atto eccedente l'ordinaria amministrazione, il consenso di entrambi i genitori è elemento necessario e presupposto legittimante³⁴. In caso contrario, devono ritenersi violati i diritti all'immagine e alla riservatezza del minore e il genitore che non ha espresso il consenso alla pubblicazione del suddetto contenuto potrà agire in sede giudiziale per l'adozione dei provvedimenti ritenuti più idonei. Nello specifico, oltre all'applicazione di una misura inibitoria che imponga il divieto di diffondere l'immagine del minore³⁵ e addirittura la rimozione del materiale già pubblicato³⁶, potrà chiedere ai gestori dei motori di ricerca la deindicizzazione di informazioni relative al minore stesso³⁷, nonché il risarcimento degli eventuali danni, patrimoniali o meno, arrecatigli³⁸.

33. Cfr. in tal senso Tribunale civile di Trani, ord., 7 settembre 2021.

34. Cfr. Tribunale civile di Pisa, 18 gennaio 2023, n. 95, che, nell'ambito di un procedimento di separazione coniugale, ordina ad entrambi i genitori la cancellazione delle foto del figlio minore pubblicate sui social networks senza il consenso dell'altro genitore. Cfr. anche Tribunale civile di Trani, 7 settembre 2021, secondo cui la possibilità del genitore di visionare un determinato profilo social non equivale ad accettazione della pubblicazione di video e foto ritraenti il figlio minore.

35. L'inibitoria a tutela del diritto d'immagine del minore, ad esempio, è stata disposta in un caso deciso dal Tribunale di Mantova con sentenza 19 settembre 2017.

36. Cfr. Tribunale civile di Torre Annunziata, sez. I, 19 maggio 2022, n. 1163, che, nell'ambito di un procedimento di separazione coniugale, rigetta la richiesta avanzata da una delle parti al fine di ottenere la rimozione dai profili social dell'altro genitore delle foto ritraenti i figli minori. In particolare, il giudice rileva come la genericità dell'assunto dell'interessato, il quale non precisa di quali foto si tratti, né opera una descrizione delle stesse, né esibisce e produce le medesime, impedisce la formulazione di qualsiasi prognosi di fondatezza della richiesta.

37. Cfr. Tribunale civile di Roma, Sez. I, 23 dicembre 2017, n. 94149.

38. Cfr. Tribunale civile di Rieti, 17 ottobre 2022, n. 443, che, nell'accogliere la domanda proposta dall'attore, padre esercente la responsabilità genitoriale sui figli minori, volta all'accertamento della responsabilità extracontrattuale della convenuta, zia di quest'ultimi, responsabile per aver pubblicato, senza l'autorizzazione paterna, sul proprio profilo Facebook numerose fotografie ritraenti i suddetti minori, ha condannato la convenuta a corrispondere una somma a titolo di risarcimento del danno non patrimoniale subito dai minori. Più nello specifico, il giudice ha sottolineato come il diritto all'immagine della persona fisica rientri nell'ambito dei diritti inviolabili dell'uomo, riconosciuti e garantiti dall'art. 2 Cost., che sancisce la libertà di autodeterminazione della persona in ordine alle proprie scelte esistenziali, tra le quali rientra quella consistente nel rendere o meno accessibile a terzi una fotografia che la ritrae. Il giudice evidenzia anche come tale diritto costituisca, altresì, una proiezione del diritto alla privacy, inteso come un diritto all'intimità della propria sfera riservata, anch'esso evidentemente

Per rinforzare l'efficacia dell'inibitoria, peraltro, è possibile chiedere al giudice di applicare una *astreinte*, ossia di fissare la somma di denaro dovuta dall'obbligato per ogni violazione o inosservanza successiva ovvero per ogni ritardo nell'esecuzione del provvedimento (art. 614-*bis* c.p.c.)³⁹.

5. La disciplina sul cyberbullismo

Altro fenomeno degno di attenzione – in quanto particolarmente insidioso, oltretutto molto diffuso – è quello del cyberbullismo, rispetto al quale il legislatore è intervenuto con la l. 29 maggio 2017 n. 71, recante “Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo”⁴⁰.

In particolar modo, ai sensi dell'art. 1, co. 2 «per “cyberbullismo” si intende qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo».

Nella sua configurazione legislativa, la fattispecie in questione è connotata da tre elementi

fondamentali, trattandosi di un illecito: a) soggettivamente qualificato dal punto di vista del soggetto passivo, necessariamente individuato in un minore o in un familiare del minore; b) tipicamente doloso e strumentalmente tipizzato; c) necessariamente commesso attraverso l'uso di strumenti digitali. Quanto, invece, all'elemento oggettivo, dalla disposizione sopra riportata – che, a ben vedere, prende in considerazione un eterogeneo elenco di condotte che appaiono accomunate «solo da un criterio teleologico implicito e cioè dalla finalità oppressiva e vessatoria che costituisce il minimo comune denominatore di ogni atteggiamento del bullo»⁴¹ – emerge chiaramente come l'effettivo inquadramento del fenomeno in questione sia tutt'altro che semplice.

Ciò che, comunque, preme sottolineare è che l'impianto edificato dal legislatore mostra una particolare predilezione verso misure educative e preventive, relegando, invece, in posizione marginale il momento sanzionatorio-repressivo⁴². Ciò emerge chiaramente sin dall'art. 1, co. 1, della legge *de qua*, ove è chiarito come la finalità perseguita sia quella di «prevenire e contrastare i fenomeni del bullismo e del cyberbullismo in tutte le loro manifestazioni, in particolare con azioni di carattere preventivo e con una strategia di attenzione e tutela nei confronti dei minori, sia nella posizione di vittime sia in quella di responsabili di illeciti, privilegiando azioni di carattere formativo ed educativo e assicurando l'attuazione degli interventi,

tutelato dal citato art. 2 Cost. nella misura in cui l'individuo è libero di decidere autonomamente se divulgare o meno a terzi le informazioni che lo riguardano.

39. Tale misura, ad esempio, è stata disposta in un caso deciso dal tribunale di Roma con sentenza 23 dicembre 2017, n. 94149.

40. A tal proposito, cfr. BENEDETTI 2023, p. 225 ss.; PERSIO 2019; BOCCHINI-MONTANARI 2018; OROFINO-PIZZETTI 2018.

41. BOCCHINI-MONTANARI 2018, p. 355.

42. A tal proposito, è interessante osservare quanto previsto dall'art. 5, co. 1, legge *de qua*, ove è stabilito che «Salvo che il fatto costituisca reato, il dirigente scolastico che, nell'esercizio delle sue funzioni, venga a conoscenza di atti di cui all'art. 1, realizzati anche in forma non telematica, che coinvolgano studenti iscritti all'istituto scolastico che dirige (...) informa (...) tempestivamente i genitori dei minori coinvolti o i soggetti esercenti la responsabilità genitoriale su di essi e promuove adeguate iniziative di carattere educativo nei riguardi dei minori medesimi, anche con l'eventuale coinvolgimento del gruppo costituente la classe in percorsi di mediazione scolastica». Solamente laddove le iniziative di carattere educativo adottate dall'istituzione scolastica non abbiano prodotto esito positivo, ovvero dinnanzi a casi particolarmente gravi o a condotte reiterate, il dirigente scolastico è chiamato a riferire alle autorità competenti (la Procura della Repubblica presso il Tribunale per i minorenni) anche per l'eventuale attivazione delle misure rieducative di cui all'art. 25 del regio decreto-legge 20 luglio 1934, n. 1404, convertito, con modificazioni, dalla l. 27 maggio 1935, n. 835.

senza distinzione di età, nell'ambito delle istituzioni scolastiche, delle organizzazioni degli enti locali, sportive e del Terzo settore che svolgono attività educative, anche non formali, e nei riguardi dei soggetti esercenti la responsabilità genitoriale, cui incombe l'obbligo di orientare i figli al corretto utilizzo delle tecnologie e di presidiarne l'uso»⁴³.

È rilevante osservare, dunque, come, a fronte della complessità e della specificità del fenomeno, la l. n. 71/2017 adotti un approccio che può definirsi duplice, individuando, da un lato, misure volte ad apprestare una tutela immediata (in forma specifica) all'immagine del minore, dall'altro, iniziative tese a prevenire il verificarsi di episodi illeciti e a sensibilizzare i minori sul tema, mediante il coinvolgimento di una pluralità di soggetti⁴⁴.

Quanto al primo aspetto, è opportuno evidenziare come l'art. 2, co. 1, prevede che «Ciascun minore ultraquattordicenne, nonché ciascun genitore o soggetto esercente la responsabilità del minore che abbia subito taluno degli atti di cui all'art. 1, comma 2, della presente legge (...) può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi altro dato personale del minore, diffuso nella rete Internet, previa conservazione dei dati originali (...)». Il secondo comma del medesimo articolo, poi, al fine di assicurare effettività e tempestività alla tutela inibitoria ivi disciplinata prevede che: «Qualora, entro le ventiquattro ore successive al ricevimento dell'istanza di cui al comma 1, il soggetto responsabile non abbia comunicato di avere assunto l'incarico di provvedere all'oscuramento, alla rimozione o al blocco richiesto, ed entro quarantotto ore non vi abbia provveduto, o comunque nel caso in cui non sia possibile identificare il titolare del trattamento o il gestore del sito internet o del social media, l'interessato può rivolgere analoga richiesta, mediante segnalazione o reclamo, al Garante per la protezione dei dati personali, il quale, entro quarantotto

dal ricevimento della richiesta, provvede ai sensi degli articoli 143 e 144 del citato decreto legislativo 30 giugno 2003, n. 196»⁴⁵.

Si tratta, in sostanza, di un'inedita forma di rimedio funzionale ad una rapida, efficace ed effettiva tutela della dignità del minore, che si traduce nella rimozione, da parte di piattaforme web, *hosting provider* e più generici gestori del sito (per la cui definizione si rimanda al co. 3 dell'art. 1), dei contenuti attraverso i quali si concretano le condotte attraverso le quali si manifesta l'episodio di cyberbullismo⁴⁶.

Quanto, invece, alle iniziative tese alla prevenzione, anzitutto rileva l'art. 4 che prevede l'adozione, da parte del Ministero dell'Istruzione, dell'Università e della Ricerca, sentito il Dipartimento per la giustizia minorile e di comunità del Ministero della Giustizia, di apposite «linee di orientamento» (da aggiornarsi con cadenza biennale), recanti, tra le altre cose, l'indicazione delle procedure per la prevenzione e il contrasto del bullismo e del cyberbullismo nelle scuole, anche attraverso il sostegno della Polizia postale e delle comunicazioni. Tali linee di orientamento, in particolare, includono un piano destinato a fornire al personale scolastico una formazione mirata, prevedono la partecipazione di un apposito referente per ogni autonomia scolastica, cui è attribuito il compito di coordinare le iniziative adottate per la prevenzione e il contrasto del fenomeno, nonché la promozione di un ruolo attivo degli stessi studenti e di ex studenti e la previsione di misure di sostegno e rieducazione dei ragazzi coinvolti nei fatti.

Le istituzioni scolastiche, peraltro, sono chiamate a promuovere l'educazione all'uso consapevole della rete Internet e ai diritti e doveri connessi all'utilizzo delle tecnologie informatiche, quale elemento trasversale alle diverse discipline curriculari, oltreché ad adottare, nell'ambito della propria autonomia, un apposito codice interno per la prevenzione e il contrasto dei fenomeni in questione e

43. L'art. 1, co. 1, della legge 29 maggio 2017, n. 71 è stato così modificato dalla legge 17 maggio 2024, n. 70.

44. Cfr. BENEDETTI 2023, p. 230.

45. In dottrina è stato evidenziato come in materia non solo risultava discussa l'applicabilità al caso di specie della disciplina prevista dal d.lgs. 9 aprile 2003, n. 70 – la giurisprudenza non essendo univoca nel considerare o meno le piattaforme del c.d. web 2.0 hosting provider in senso stretto – ma altresì del tutto indeterminata la procedura volta all'oscuramento, rimozione o blocco dei contenuti illeciti diffusi dal cyberbullo in rete. A tal proposito, cfr. BOCCHINI-MONTANARI 2018, p. 350.

46. Cfr. BENEDETTI 2023, p. 366 ss.

istituire un tavolo permanente di monitoraggio al quale sono chiamati a sedere rappresentanti degli studenti, degli insegnanti, delle famiglie ed esperti del settore.

6. L'importanza di impartire un'adeguata educazione civica al digitale

Alla luce di quanto detto sopra – la disciplina in materia di cyberbullismo è emblematica in tal senso – risulta evidente l'importanza di un'adeguata attività preventiva che, tra le altre cose, si ponga l'obiettivo di far maturare una diffusa consapevolezza circa i pericoli cui chi naviga in Internet va incontro.

Alla luce di un sistema che – nonostante il d.lgs. 101/2018, come già detto, abbia fissato a quattordici anni l'età minima per poter prestare validamente il consenso al trattamento dei dati personali⁴⁷ – impone ai genitori degli obblighi di controllo sull'operato digitale dei figli, emerge chiaramente la delicatezza del ruolo ricoperto dai primi che, peraltro, spesso e volentieri non conoscono il funzionamento dei nuovi strumenti di comunicazione, così come non padroneggiano quelle soluzioni tecniche che la gran parte degli operatori offre allo scopo di accompagnare i giovani nell'esperienza digitale (es. sistemi di controllo parentale,

limitazione/disabilitazione di applicazioni e funzionalità potenzialmente dannose, ecc).

Sarebbe utile, allora, pensare a dei veri e propri piani formativi, aggiuntivi o comunque integrativi rispetto a quelli già concepiti dal legislatore⁴⁸, rivolti sia ai minori che ai genitori, al duplice fine di informare e responsabilizzare entrambe le categorie di soggetti circa il corretto modo di utilizzare la rete e, in particolare, i *social media network*.

Le istituzioni – oltre ad adoperarsi per superare il divario digitale, ad esempio garantendo la fornitura di un accesso alla rete gratuito e sicuro per i minorenni in luoghi pubblici dedicati e l'investimento in politiche e programmi che supportino l'accesso a Internet a prezzi accessibili per i più giovani – dovrebbero adottare tutte le misure necessarie al fine di assicurare un uso consapevole delle tecnologie digitali nei contesti educativi, nella comunità e a casa. Esse dovrebbero garantire che il superiore interesse della persona minore d'età – nel tenere in considerazione il quale dovrebbero fare riferimento a tutti i suoi diritti, compresi, da un lato, quello di cercare, ricevere e diffondere informazioni, nonché, dall'altro lato, quello di essere protetti dai rischi che ne minacciano uno sviluppo sano – assuma rilevanza primaria in tutte le azioni riguardanti la fornitura, la regolamentazione, la

47. In dottrina si è evidenziato come tale aspetto ponga delle questioni di compatibilità con gli obblighi di controllo che l'ordinamento prevede in capo ai genitori del fanciullo. In tal senso, cfr. BENEDETTI 2023, p. 236.

48. Con la legge 20 agosto 2019, n. 92 (*Introduzione dell'insegnamento scolastico dell'educazione civica*), a partire dall'anno scolastico 2020-2021, è stato (re)introdotta l'insegnamento trasversale dell'educazione civica nel primo e secondo ciclo d'istruzione. Tra i nuclei tematici v'è anche quello della Cittadinanza digitale, cui è dedicato l'art. 5 della legge. In particolare, l'insegnamento mira a sviluppare con gradualità, tenendo conto dell'età degli alunni e degli studenti, le seguenti abilità: a) analizzare, confrontare e valutare criticamente la credibilità e l'affidabilità delle fonti di dati, informazioni e contenuti digitali; b) interagire attraverso varie tecnologie digitali e individuare i mezzi e le forme di comunicazione digitali appropriati per un determinato contesto; c) informarsi e partecipare al dibattito pubblico attraverso l'utilizzo di servizi digitali pubblici e privati; ricercare opportunità di crescita personale e di cittadinanza partecipativa attraverso adeguate tecnologie digitali; d) conoscere le norme comportamentali da osservare nell'ambito dell'utilizzo delle tecnologie digitali e dell'interazione in ambienti digitali, adattare le strategie di comunicazione al pubblico specifico ed essere consapevoli della diversità culturale e generazionale negli ambienti digitali; e) creare e gestire l'identità digitale, essere in grado di proteggere la propria reputazione, gestire e tutelare i dati che si producono attraverso diversi strumenti digitali, ambienti e servizi, rispettare i dati e le identità altrui; utilizzare e condividere informazioni personali identificabili proteggendo se stessi e gli altri; f) conoscere le politiche sulla tutela della riservatezza applicate dai servizi digitali relativamente all'uso dei dati personali; g) essere in grado di evitare, usando tecnologie digitali, rischi per la salute e minacce al proprio benessere fisico e psicologico; essere in grado di proteggere sé e gli altri da eventuali pericoli in ambienti digitali; essere consapevoli di come le tecnologie digitali possono influire sul benessere psicofisico e sull'inclusione sociale, con particolare attenzione ai comportamenti riconducibili al bullismo e al cyberbullismo.

progettazione, la gestione e, soprattutto, l'utilizzo dell'ambiente digitale.

Sarebbe importante, dunque, fornire un supporto effettivo che consenta anche ai genitori e a coloro che si prendono cura del minore di accompagnarlo – sempre nel rispetto dell'autonomia del ragazzo e del suo bisogno di privacy – nell'acquisizione dell'alfabetizzazione digitale e di una piena consapevolezza delle potenzialità positive e negative del Web.

A tal proposito, si segnala che di recente un apposito Tavolo tecnico istituito con decreto del Ministro della giustizia del 21 giugno 2021, alla luce di un'attenta analisi del fenomeno della presenza dei minori sui social network, ha evidenziato, tra le altre cose, proprio l'esigenza di promuovere campagne di comunicazione e sensibilizzazione sui rischi del Web, al fine di incrementare il livello diffuso di educazione al digitale⁴⁹.

La strategia principale per diminuire i rischi di abusi o, più in generale, di comportamenti errati è risultata quella di stimolare e fortificare le capacità critiche di analisi e gestione dei mezzi digitali. A tal fine, si è evidenziata l'opportunità di segmentare in diversi target l'insieme degli utenti, al fine di sviluppare e impiegare canali e codici comunicativi adeguati alle diverse caratteristiche che essi presentano.

Quanto agli adulti, ad esempio, è stata sottolineata proprio la necessità di fornire loro un sostegno, al fine di far loro acquisire e sviluppare quelle conoscenze tecnologiche necessarie per assistere i minorenni in relazione all'ambiente digitale, nonché allo scopo di far maturare piena consapevolezza circa l'impatto che le tecnologie digitali possono avere sul naturale ed equilibrato sviluppo psicofisico dei ragazzi. Obiettivi, questi, che appaiono impossibili da raggiungere ricorrendo unicamente alle consuete campagne istituzionali di sensibilizzazione diffuse attraverso i media tradizionali, i quali vanno incontro a un crescente "disaffezionamento" da parte degli utenti. Al contrario, forse

sarebbe opportuno adoperare, attraverso una collaborazione con gli stessi operatori della rete e dei social network, proprio quei canali e quegli strumenti digitali sempre più diffusi anche tra gli adulti⁵⁰. Particolare attenzione dovrebbe, senz'altro, essere prestata ai genitori e a coloro che si prendono cura dei minorenni che si trovano in situazioni svantaggiate o vulnerabili.

Quanto, invece, al pubblico dei minorenni, si ritiene opportuno procedere con ulteriori segmentazioni in ragione delle sensibili differenze cognitive e comportamentali legate alle diverse classi di età. È importante rispettare l'evoluzione delle capacità del minorenne, assumendola quale criterio-guida nell'affrontare il processo volto ad una loro graduale acquisizione di competenze. I rischi e le opportunità associati al coinvolgimento dei minorenni nell'ambiente digitale, in effetti, cambiano a seconda della fase di sviluppo, cosicché la progettazione di misure di protezione o di facilitazione del loro accesso alla rete dovrebbe essere "cucita su misura" tenendo conto delle specificità e delle esigenze che connotano le differenti fasce di età.

Per quel che riguarda, ad esempio, il segmento degli studenti delle scuole secondarie di primo grado – che possono considerarsi sufficientemente capaci di sviluppare una corretta comprensione dei messaggi dedicati al tema – si ritiene necessario andar oltre le consuete formule di comunicazione scolastica-istituzionale ed evitare toni burocratici o paternalistici. Ciò non vuol dire escludere completamente gli insegnamenti e i media tradizionali, ma è chiaro che non si può prescindere dalle forme di comunicazioni ad oggi per loro più familiari e rappresentative, inserendo nei piani comunicativi-formativi figure che fanno parte del loro mondo e che, proprio per questo, risultano in grado di interpretare efficacemente le loro istanze e i loro bisogni. Si dovrebbe, peraltro, rispondere anche alle esigenze dei minorenni in situazioni svantaggiate o di vulnerabilità, fornendo informazioni a

49. Si tratta del *Tavolo tecnico sulla tutela dei diritti dei minori nel contesto dei social networks, dei servizi e dei prodotti digitali in rete*. In data 10 maggio 2022, il Tavolo ha licenziato la *Relazione finale*, consultabile sul sito del Ministero della Giustizia, dando conto dei risultati dei lavori.

50. In questo senso, dalla Relazione si evince come il Tavolo tecnico abbia teorizzato la realizzazione di una piattaforma online specificatamente dedicata agli adulti, da sviluppare in collaborazione tra istituzioni, media e operatori, per far fronte alle esigenze formative dei minori anche attraverso il contributo di esperti del mondo digitale, sociologi, psicologi, pedagoghi.

loro misura che, se necessario, vengano tradotte nelle principali lingue minoritarie.

In altri termini, occorrerebbe fondare questo percorso di sensibilizzazione su una nuova

modalità di dialogo per interagire sia con i genitori che con i ragazzi rendendoli pienamente partecipi degli itinerari da intraprendere.

Riferimenti bibliografici

- AUTORITÀ GARANTE PER L'INFANZIA E L'ADOLESCENZA (a cura di) (2019), *La Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza. Conquiste e prospettive a 30 anni dall'adozione*, 2019
- A.M. BENEDETTI (2023), *Minori "buoni" e minori "cattivi" nella nuova disciplina sul cyberbullismo*, in E. Ceccherini, F. Brunetta d'Usseaux (a cura di), "Best interest(s) of the child", Editoriale Scientifica, 2023
- M. BESSONE (1976), *Art. 30-31*, in G. Branca (a cura di), "Commentario della Costituzione, Rapporti etico-sociali", Zanichelli, 1976
- M. BIANCA (a cura di) (2021), *Best interest of the child*, Sapienza Università Editrice, 2021
- C.M. BIANCA (2021-A), *Diritto civile. 5, La responsabilità*, Giuffrè, 2021
- R. BOCCHINI, M. MONTANARI (2018), *Le nuove disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo (l. 29 maggio 2017, n. 71)*, in "Le Nuove leggi civili commentate", 2018, n. 2
- E. CECCHERINI, F. BRUNETTA D'USSEAU (a cura di) (2023), *Best interest(s) of the child, Una delicata e controversa declinazione*, Editoriale Scientifica, 2023
- E. DI NAPOLI (2023), *La dimensione internazionale e sovranazionale del superiore interesse della persona di minore età*, in E. Ceccherini, F. Brunetta d'Usseaux (a cura di), "Best interest(s) of the child, Una delicata e controversa declinazione", Editoriale Scientifica, 2023
- G. FERRANDO (1998), *Diritti e interesse del minore tra principi e clausole generali*, in "Politica del diritto", 1998, n. 1
- E. LAMARQUE (2006), *Art. 30*, in R. Bifulco, A. Celotto, M. Olivetti (a cura di), "Commentario alla Costituzione", Utet Giuridica, 2006
- M. MAGLI, G. SPADARO (2020), *Diritti dei minori e rapporti tra le fonti del diritto internazionale*, in "Il diritto vivente", 24 giugno 2020
- M. OROFINO, F.G. PIZZETTI (2018) (a cura di), *Privacy, minori e cyberbullismo*, Giappichelli, 2018
- P.T. PERSIO (2019), *Il contrasto al "cyberbullismo" nella legge n. 71/2017 tra finalità di prevenzione ed esigenze di repressione*, in "La Giustizia Penale", 2019, n. 1
- S. PITTO (2023), *La giustizia non ha età. Il principio del best interest of the child per una giustizia "a misura di bambino"*, in E. Ceccherini, F. Brunetta d'Usseaux (a cura di), "Best interest(s) of the child, Una delicata e controversa declinazione", Editoriale Scientifica, 2023
- C. RAVERA (2019), *Minori e internet: quando i genitori devono vigilare*, in "ilFamiliarista.it", 20 marzo 2019



BENEDETTA AGOSTINELLI

Autonomia e controllo dei minori on line. I nuovi confini della responsabilità genitoriale

La responsabilità genitoriale, che ha superato la potestà, è situazione giuridica complessa idonea a riassumere i doveri, gli obblighi e i diritti derivanti per il genitore dalla filiazione, tra i quali emerge quello di educare. I minori sono particolarmente esposti sul Web, luogo virtuale dove sviluppare la propria personalità ma anche pieno di rischi legati a una navigazione non sempre consapevole e sicura. A 14 anni, poi, il consenso al trattamento dei dati personali nei servizi della società dell'informazione (quindi anche social network) viene prestato direttamente dal minore e i sistemi di *parental control*, se attivati, vengono interrotti bruscamente e non possono essere mantenuti dai genitori senza la volontà del minore. Ciò riduce la capacità di controllo e di indirizzo dei genitori, che devono per primi rispettare la privacy dei figli, evitando di sovraesporli, e incide sull'esercizio stesso della responsabilità genitoriale.

Responsabilità genitoriale – Minori – Educazione – Consenso – Sharenting

Autonomy and control of minors online. The new borders of parental responsibility

Parental responsibility is a complex legal situation that summarizes the duties and rights of parents, among which emerges education. Minors are particularly exposed on the Web, a virtual place where they can develop their own personality but also full of risks related to a not always conscious and safe navigation. At 14, the consent to the processing of personal data in information society services (and therefore also social networks) is given directly by the child and parental control systems, if activated, are abruptly interrupted and cannot be maintained by the parents without the will of the child. This reduces the ability of parents – who must first respect the privacy of their children, avoiding overexposing them in the web – to control and guide, and affects the very exercise of parental responsibility.

Parental Responsibility – Minors – Education – Consent – Sharenting

L'Autrice è professoressa ordinaria di Diritto privato presso l'Università degli Studi Roma Tre

Questo contributo fa parte della sezione monografica *Minori e Internet* a cura di Carlo Colapietro e Antonio Iannuzzi

SOMMARIO: 1. La responsabilità genitoriale, il potere di controllo, il diritto-dovere di educare. – 2. Il “consenso digitale” dei minori in rete. – 3. I sistemi di *parental control*. – 4. La tutela *dei* genitori e la tutela *dai* genitori: il fenomeno dello *sharenting*. – 5. Conclusioni: nuovi confini per la responsabilità genitoriale.

1. La responsabilità genitoriale, il potere di controllo, il diritto-dovere di educare

Assodata l'ingombrante presenza delle nuove tecnologie e dei mezzi di interconnessione digitale nella vita dei giovani e – non meno – di chi giovane non è più, l'argomento degli effetti e dei rischi di tale presenza, lungi dall'essere tema di rilevanza esclusivamente sociologica o addirittura antropologica, investe e interroga direttamente il diritto e, segnatamente, il diritto privato di famiglia.

Non è dunque corretto pensare che la regolazione dell'uso (e financo della definizione e costruzione) dei dispositivi o delle applicazioni che rendono possibile tale uso sia una (mera) regolazione – pur giuridica – della tecnologia: se certamente è anche questo, quando l'uso è in particolare posto in essere attivamente – o riguarda passivamente – un minore è precipuamente una questione di responsabilità genitoriale.

Il minore, infatti, non è un'entità giuridica astratta, o un soggetto giuridico con la peculiarità della minore età: è, prima di tutto e in modo qualificante, un figlio (nella normalità dei casi, e in quelli eccezionali è comunque dotato dalla legge di referenti titolari della responsabilità genitoriale, come ad esempio un tutore).

Questo “ruolo” giustifica la presenza, accanto al corredo di norme a lui dedicate quale fruitore della rete naturalmente più vulnerabile, della tutela scaturente dal rapporto di filiazione e quindi chiama in causa anche il ruolo, speculare ed insostituibile dei genitori.

Sin da subito si evidenzia come, dunque, sia la responsabilità genitoriale, di cui all'art. 316 c.c., il vero e centrale ambito in cui inscrivere anche il delicato e attualissimo problema dell'uso (o abuso) della rete da parte dei minori e del relativo controllo esterno.

Non a caso l'intero capo I del titolo IX del libro I del codice civile è attraversato dal “filo rosso” della responsabilità genitoriale.

Nella sua orbita sono *naturaliter* attratti i diritti dei figli (art. 315-*bis* c.c.) che costituiscono, sul fronte opposto, doveri a riempire di contenuto la posizione dei genitori, prescrivendo il *quid* – se non il *quomodo* – della loro condotta (mantenere, istruire, educare, assistere moralmente).

L'assetto attuale è l'approdo di un lungo percorso di ridefinizione della relazione filiale che ha a mano a mano recepito in via positiva le trasformazioni culturali maturate nella società.

Innanzitutto occorre ricordare come la sua precedente, fondamentale, tappa – che ha consentito il necessario adeguamento anche al dettato costituzionale (artt. 29, 30 Cost.) – abbia interessato in primo luogo la relazione orizzontale tra genitori.

Con la riforma del diritto di famiglia del 1975, infatti, la potestà *patria* che palesamente sconfessava “l'uguaglianza morale e giuridica” dei coniugi (sulla quale è ordinato il matrimonio *ex* art. 29 Cost.), è divenuta *genitoriale* e da quella data viene in qualche misura sfrondata dei più anacronistici profili di autorità e soggezione del figlio¹, eredità storica della tradizione ottocentesca, a sua

1. Basti pensare all'art. 319 c.c., abrogato appunto nel 1975, che, rubricato “Cattiva condotta del figlio”, consentiva al padre che tale condotta non riuscisse a “frenare”, di collocare il figlio in un istituto di correzione.

volta radicata, retrospettivamente, nell'archetipo del *paterfamilias* del diritto romano e nella logica dominicale ad esso sottesa².

Sebbene l'introduzione innovativa dell'esercizio "in comune" della potestà del 1975 avesse cancellato dall'art. 316 c.c. previgente l'ingiustificabile disparità di posizioni tra madre e padre³, era stata conservata la previsione del possibile intervento del solo padre per adottare provvedimenti "urgenti e indifferibili" in caso di imminente pericolo di un grave pregiudizio per il figlio.

Anche quest'ultimo retaggio patriarcale è venuto meno con la riforma della filiazione di cui alla l. n. 219/2012 e successivo d.lgs. n. 154/2013, imprimendosi così un "ulteriore sviluppo alla prospettiva «puerocentrica» inaugurata formalmente con la riforma del diritto di famiglia del 1975"⁴.

Proprio la maggiore elasticità del nuovo istituto – la responsabilità genitoriale – quindi consente, più agevolmente di prima, di ricondurre ad una complessiva funzione di *cura* tutti gli ambiti di competenza genitoriale.

La stessa Relazione al d.lgs. n. 154/2013 precisa, peraltro, che la nuova responsabilità si presenta come "situazione giuridica complessa idonea a riassumere i doveri, gli obblighi e i diritti derivanti per il genitore dalla filiazione", in quanto tale più estesa della potestà, e che la soggezione del figlio si tramuta in "assunzione di responsabilità da parte dei genitori" nei suoi confronti, come emerge

appunto dalla "modifica terminologica" che "attuata in considerazione della evoluzione socioculturale, prima che giuridica, dei rapporti tra genitori e figli (...) dà risalto alla diversa visione prospettica che nel corso degli anni si è ormai sviluppata ed è ormai da considerare patrimonio condiviso: i rapporti genitori-figli non devono più essere considerati avendo riguardo al punto di vista dei genitori, ma occorre porre in risalto il superiore interesse dei figli minori".

Su questa "trasformazione" della potestà in responsabilità molto è stato detto, proprio muovendosi specialmente dal cambio di denominazione che ha suscitato anche perplessità e critiche.

Il termine prescelto è l'esito della traduzione dalla *parental responsibility* di fonti straordinarie, in particolare il Reg. CE n. 2201/2013 relativo alla competenza, al riconoscimento e all'esecuzione delle decisioni in materia matrimoniale e in materia di responsabilità genitoriale (c.d. *Bruxelles II bis*) oltretutto già la Dichiarazione ONU dei diritti del fanciullo del 1959⁵. La Relazione illustrativa della riforma chiarisce che l'abbandono della nozione di potestà intende valorizzare il profilo della "assunzione di responsabilità da parte dei genitori nei confronti del figlio".

Alcune opinioni favorevoli hanno ritenuto il passaggio consoni ai tempi e di portata significativa: archiviato un istituto anacronistico⁶, è tramontato lo schema potestà-soggezione, espressione

Sulla trasformazione della potestà in responsabilità genitoriale, sia consentito rinviare a AGOSTINELLI 2024, p. 98 ss.

2. Espressione di un'idea di potere, comando, supremazia, da un lato, e soggezione, dall'altro: v. DOGLIOTTI 2019, p. 137 ss. Un approfondito excursus storico della condizione dell'infanzia dall'antica Grecia sino all'avvento dell'"era della cura e dell'ascolto del minore" è offerto da PALAZZO 2013, p. 509 ss. Di patria potestà modellata, nei codici liberali, "sullo stampo del diritto di proprietà" parla Mengoni 1982, p. 1119, «giusta l'antica idea del figlio "naturaliter aliquid patris", poi sublimata dalla cultura borghese nella figura del padre che lavora per i figli e si giustifica in essi».
3. Ma sull'impiego persistente della locuzione ormai superata di "patria potestà" talvolta da parte della giurisprudenza talaltra addirittura del legislatore, quale sintomo di un non definitivo superamento di un anacronismo normativo e sociale, v. MONTECCHIARI 2006, p. 7 ss.
4. "Tentativo meritorio" ad avviso di RUSCELLO 2015, p. 717; RUSCELLO 2012. Sullo spirito della riforma del diritto di famiglia del 1975 rispetto alla posizione del minore v. GIARDINA 1977, p. 1352 ss.; GIARDINA 1990.
5. Cfr. CIANCI 2014, p. 89 ss.; GORASSINI 2014, p. 91 ss.
6. V. AL MUREDEN 2014; DOGLIOTTI 2019, p. 138; BIANCA 2023, p. 378, ritiene che si sia voluto «sottolineare il mutamento dell'antica concezione dell'autorità spettante ai genitori e, in passato, al capo della famiglia»; concezione che «ha ormai lasciato il posto all'idea che i genitori sono titolari di un ufficio, che si deve esercitare nell'interesse della prole». Per SALANTRO 2014, p. 540: «è stato adeguata al significato corrente della disciplina costituzionale

della visione autoritaria delle relazioni familiari, a sua volta specchio, in origine, della logica dominicale di cui s'è detto⁷.

Altra parte della dottrina, di contrario avviso, ritiene la modifica prevalentemente lessicale e non di sostanza, ed evidenzia anche che il "trapianto"⁸ basato su di un equivoco di fondo relativo alla scelta del nuovo lemma inadatto allo scopo genera una serie di incongruenze semantiche, come la difficoltà di predicare rispetto ad una responsabilità (a differenza di un potere) un esercizio o una decadenza⁹.

Considerando tuttavia che le parole, tanto più il *nomen* degli istituti, hanno un loro peso oltreché un loro significato, la scelta del riformatore non solo di eliminare la "potestà" ma anche di optare per la "responsabilità" rende il senso del passaggio da potere a funzione, con esplicito riferimento all'interesse del relativo esercizio: quello del figlio.

Certamente l'opzione innovatrice ha enfatizzato – questo è innegabile – la pregnanza del nuovo ruolo dei genitori, di sicuro avvertito socialmente e tradotto ora in un linguaggio normativo più adatto ed

attuale, rimodellando la lettura della relazione genitoriale e depurandola dei tratti gerarchici più retrivi.

Tuttavia, e fermo quanto sopra, non possono dirsi stravolti i connotati fondamentali della componente potestativa, riconducibile all'esercizio di potere nell'interesse altrui e, per una buona parte, in sua sostituzione.

Sebbene riletta sotto la nuova luce, tale componente è insopprimibile e irrinunciabile, proprio per il funzionamento stesso dell'istituto che resta uno strumento di attuazione dei doveri attribuiti ai genitori¹⁰.

Posto che il legislatore non ha voluto fornire una definizione puntuale, onde lasciare la nozione suscettibile di venire "riempita di contenuti a seconda dell'evoluzione socio-culturale dei rapporti genitori-figli"¹¹, il suo nucleo consiste, infatti, – e non potrebbe essere diversamente pena lo svuotamento quasi totale dell'istituto – nello svolgimento di quei diritti e doveri che già prima incombevano ai titolari della potestà¹² e nel rispetto di quei medesimi indici identitari personali (capacità, inclinazioni naturali e aspirazioni) che infatti campeggiano anche nell'art.

del rapporto tra genitori e figli la denominazione dell'istituto, abbandonando quella di "potestà", evocativa di un rapporto di subordinazione del figlio nei confronti dei genitori, e accogliendo quella di "responsabilità", che suggerisce la funzione servente del ruolo genitoriale rispetto all'interesse dei figli».

7. Osservava, del resto, RUSCELLO 2006, p. 11: «La famiglia che nasce con il codice del 1942 è una famiglia che come tutto l'impianto normativo, nasce già vecchia».
8. SCHLESINGER 2014, p. 445, invita «a guardare senza eccessiva enfasi ad un "calco" lessicale forse non pienamente riuscito». Il mutamento è soltanto formale agli occhi di RUSCELLO 2015, p. 718. Per BUSNELLI 2016, p. 1473, si è trattato di «un maldestro e fuorviante fraintendimento della norma in cui la Convenzione di New York sui diritti del fanciullo sancisce "la responsabilità, il diritto e il dovere dei genitori" (art. 5). Ma è, forse, più semplicemente un richiamo irresistibile, quanto inconfidente, alla clausola generale dei best interests of the child, in ragione della quale – aggiunge sconsideratamente la menzionata Relazione – "i rapporti genitori figli non devono più essere considerati avendo riguardo al punto di vista dei genitori"».
9. Ai rilievi di DE CRISTOFARO 2014, rispetto all'improprietà del lessico, alla vaghezza del contenuto, nonché all'eccesso di delega cui sarebbe incorso il riformatore, replica BIANCA 2015, evidenziando che la scelta del termine è stata adottata proprio «per sottolineare il mutamento del nuovo istituto non più improntato all'antica concezione dell'autorità che connotava l'antica potestà ma all'idea di un ufficio incentrato sulla posizione del figlio e attribuito nel suo interesse e delineato, come richiesto dalla legge delega, quale "nuovo aspetto ossia nuovo volto dell'antica potestà"».
10. In questo senso DOGLIOTTI 2019. Per GORASSINI 2012, p. 413, nella responsabilità si trova «proprio il meccanismo strutturale primordiale dell'autorità collegata ai rapporti familiari, rapporti nei quali, per necessità, almeno 1 dei due genitori deve essere x un altro, il figlio, e che rende il fenomeno d'insieme familiare, un fenomeno unico».
11. V. ancora la Relazione illustrativa.
12. Ancora BIANCA 2015, p. XXXVIII, ricorda che «il significato è inscindibilmente connesso con i diritti dei figli». Il nuovo ufficio «è infatti conferito ai genitori per la realizzazione dei diritti dei figli e si determina nel suo

315-*bis* c.c., “norma-specchio”, in qualche misura, dell’art. 316 c.c.¹³.

Una volta assorbito nel sistema il (nuovo) istituto, in esso come già per il precedente si è soliti distinguere un “lato interno”, attinente alla guida, controllo e sorveglianza di una persona in divenire, qual è il figlio, corrispondente al profilo personale, ed un “lato esterno”, relativo alla rappresentanza e all’amministrazione dei beni, corrispondente al profilo patrimoniale (governato dagli artt. 320 ss.)¹⁴.

Ora, se la titolarità astratta della responsabilità genitoriale, che rappresenta “l’aspetto statico e formale”, scaturisce dalla costituzione del rapporto di filiazione, l’esercizio invece indica “l’aspetto dinamico e sostanziale”¹⁵ e la legge lo prescrive “di comune accordo” tra i genitori (art. 316 c.c.), precisando all’art. 317 c.c. che, in caso di impossibilità di un genitore, l’esercizio esclusivo spetta all’altro, rinviandosi per l’eventualità di crisi e dissolvimento della coppia, comunque configurabile, alla disciplina del capo II del medesimo titolo IX, dedicato appunto all’esercizio della responsabilità genitoriale in tale evenienza e a prescindere dal coniugio preesistente tra i genitori¹⁶.

L’art. 316 c.c. specifica all’ultimo comma che il genitore che non esercita la responsabilità genitoriale vigila sull’istruzione, sull’educazione e sulle condizioni di vita del figlio¹⁷.

Se, come detto, nella responsabilità genitoriale si distingue un profilo personale ed uno patrimoniale, il primo trova nell’art. 315-*bis* c.c. con il relativo “catalogo” di doveri genitoriali il suo naturale completamento¹⁸.

In particolare è qui da considerare il dovere di educare posto che se il generale dovere di cura si

specifica in accudimento e sostegno sotto la distinta voce “assistenza morale”, sotto quella di “educazione” va ricondotto l’insegnamento di principi e regole di comportamento che consentano lo sviluppo armonico della persona per il suo migliore inserimento nella società, a beneficio anche di quest’ultima.

La funzione educativa risente peraltro sia del mutato ruolo del figlio all’interno della compagine familiare sia dell’accelerazione dello sviluppo della sua personalità connessa all’anticipazione delle occasioni di crescita e di autodeterminazione dei minori, dato oggi comunemente registrabile ed ormai irreversibile, specie con l’avvento dell’era digitale.

Le implicazioni di tale ultimo fenomeno sociale, che vede i minori “immessi” sempre prima nel mondo degli adulti ed utilizzare le medesime modalità di comunicazione e socializzazione, sono state considerate sino ad ora prevalentemente con riguardo alla capacità d’agire e dunque all’attitudine spiccatamente negoziale sempre più precoce. Sotto altro versante, in realtà, detto fenomeno ha determinato anche l’aumento della potenzialità lesiva della loro stessa condotta (si pensi al drammatico fenomeno del cyberbullismo), proprio in ragione della incrementata possibilità di muoversi al di fuori della tradizionale sfera di controllo dei genitori.

Se, dunque, aumenta l’“esposizione” del minore al mondo esterno ed il contatto con la società (pur fatta anche di coetanei) che, in un certo senso, lo attende adulto, sollecitandolo sempre prima a diventarlo, può dirsi aumentare di riflesso il “bisogno” di educazione, quale cura mirata a fornire proprio gli strumenti per rapportarsi ad esso.

contenuto in relazione ai doveri correlativi a tali diritti». Ad avviso di RECINTO 2016, p. 62 ss., la nuova prospettiva della dinamica relazionale della responsabilità genitoriale potrebbe essere letta in chiave di obblighi di protezione, arrivando a configurarsi, in capo ai genitori, una responsabilità contrattuale.

13. Secondo BUSNELLI 2016, p. 1473, «In realtà, la nozione di “potestà genitoriale”, disinvoltamente soppressa all’ultimo memento, è ancora indispensabile, per l’interprete chiamato ad applicare le nuove norme intitolate ai “diritti e doveri del figlio”, come sintesi collaudata dei “diritti e doveri” che necessariamente devono connotare la responsabilità dei genitori, se si vuole che tale responsabilità non scada al livello di mero affare privato».

14. V., per tutti, DOGLIOTTI 2019; BIANCA 2023, p. 378.

15. LENTI 2021, p. 294.

16. Su cui v. PATTI-ROSSI CARLEO 2021.

17. Per GORASSINI 2014, p. 92, l’antica potestà, «come situazione giuridica in capo al genitore» sembra rimanere paradossalmente in questa previsione che la presuppone quale “ultima ombra”.

18. Per un approfondimento sia consentito rinviare a AGOSTINELLI 2024, p. 46 ss.

A tale processo di emancipazione sociale si accompagna allora un incremento della rilevanza del momento educativo e una sua “specializzazione” digitale, per così dire, che quindi rientra pienamente nel contenuto del relativo dovere: in altri termini, i genitori devono impartire ai figli una specifica “educazione digitale” per assolvere integralmente al loro compito¹⁹.

Se, quindi, avvertimenti e raccomandazioni da sempre rappresentano gli strumenti che i genitori impiegano per condurre la guida verso l'autonomia, ora gli stessi vanno declinati rispetto all'uso della tecnologia e in quel contesto, posto che quello è il contesto in cui i figli non solo si trovano a vivere²⁰ ma, in un'età ancora lontana dalla maggiore, si trovano a godere di un certo potere di autodeterminazione, legalmente attribuito.

2. Il “consenso digitale” dei minori in rete

L'art. 8 del Regolamento europeo per la protezione dei dati (Reg. EU 2016/679, o GDPR)²¹, infatti,

dispone che ove il trattamento preveda il consenso dell'interessato, se vi è “un'offerta diretta di servizi della società dell'informazione” ai minori, tale trattamento “è lecito ove il minore abbia almeno 16 anni”, in caso di età inferiore va prestato o autorizzato da chi esercita la responsabilità genitoriale. Il limite di questa sorta di “maggiore età digitale” può venire ulteriormente abbassato dagli Stati nazionali (ma non al di sotto dei 13 anni)²² e il legislatore italiano, col decreto di adeguamento del codice privacy²³, ha ritenuto di fissarlo nei 14 anni, stilando una norma (art. 2-*quiquies*, d.lgs. n. 193/1996)²⁴ ancora più chiara: “il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione”.

Il GDPR, peraltro, sulla scorta di una costante attenzione eurounitaria verso i minori particolarmente esposti durante la navigazione in rete, proclama uno speciale riguardo nei loro confronti al

19. Sulla necessità di una specifica “dimensione digitale” nell'educazione, da non confondere con l'educazione digitale come “complesso di regole di competenza sull'uso della rete”, v. BIANCA 2019, p. 161; PERLINGIERI 2016, p. 1332 ss.; in argomento sia consentito rinviare anche ad AGOSTINELLI 2021. Sul fronte degli studi in ambito psicologico, v., ad es., VOLPI 2017.

20. Per un dettagliato resoconto della (preoccupante) condizione dei minori on line, v. i dati recenti riportati nella Documentazione per l'esame di Progetti di legge *In materia di minori e Internet, con riferimento particolare all'accesso alle piattaforme e all'uso dell'immagine dei minori* AA.C. 1217, 1771, 1800 e 1863, da cui emerge quanto precoci e assidui frequentatori della rete siano: il 73% dei minori (tra i 6 e i 17 anni) ha dichiarato di connettersi a Internet quotidianamente e, circa i rischi della rete per i minori, il 42 per cento dei minori e il 53 per cento degli adolescenti dai 13 anni, raccontano esperienze negative gravi e ripetute.

21. Per un commento puntuale della norma si rinvia a MONTARULI 2019; SPOTO 2016; LUCCHINI GUASTALLA 2019.

22. In ciò il GDPR riproduce in sostanza la previsione del Children's Online Privacy Protection Act 1998 (Coppa), che negli USA limita il necessario parental consent al raggiungimento dei 13 anni.

23. Sull'adeguamento del “vecchio” codice privacy (d.lgs. n. 196/2003) avvenuto con il d.lgs. n. 101/2018 secondo una tecnica di novellazione assai discutibile, CUFFARO 2018-A.

24. Contro il parere del 23 maggio 2018, n. 1008, peraltro, del Garante per l'Infanzia e l'Adolescenza, che suggeriva di confermare l'opzione europea dei 16 anni, quale età più idonea a garantire un più avanzato stadio di maturazione dell'adolescente, e già stabilita, ad es., per il riconoscimento del figlio e per la cessazione dell'obbligo scolastico. Favorevole invece il Garante privacy (parere 22 maggio 2018, n. 312) per analogia con altre previsioni positive, quali l'assenso all'adozione e la promozione autonoma della tutela nei casi di cyberbullismo. Anche altri paesi hanno utilizzato la deroga: se, ad es., Germania, Lussemburgo, Paesi Bassi, Romania, Slovacchia, Ungheria, Irlanda hanno lasciato il limite dei 16 anni; Grecia, Repubblica Ceca, Slovenia, Francia l'hanno abbassato a 15 anni, mentre Austria, Bulgaria, Cipro, Lituania, Spagna, come l'Italia, a 14 anni e Belgio, Regno Unito, Svezia, Norvegia, Danimarca, Finlandia, Portogallo addirittura a quello minimo di 13 anni. In Italia, sono attualmente all'esame del Parlamento dei progetti di legge per l'innalzamento dell'età a 15 anni (A.C. 1217, A.C. 1863); a 16 anni (A.C. 1771) o addirittura per l'abrogazione dell'art. 2 quinquies cod. Privacy (A.C. 1800).

considerando 38²⁵, che li riconosce apertamente “meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali” e al considerando 58, dove si prescrive un linguaggio “semplice e chiaro che un minore possa capire facilmente” per qualsiasi informazione e comunicazione “quando il trattamento dati li riguarda”. Peraltro resta salva anche per i minori la possibilità sia di revocare il consenso dato sia di invocare il diritto all’oblio, inteso qui ed evolutosi in diritto alla cancellazione dei dati, successivamente al raggiungimento della maggiore età rispetto all’epoca in cui il consenso fu espresso (art. 17)²⁶.

L’introduzione di un “consenso digitale” anticipato rispetto alla soglia legale della maggiore età – assente nell’originaria dir. 96/46/CE in materia – ha incontrato un favore generalizzato, venendo prevalentemente letta come un passo ulteriore nella direzione di una maggiore autonomia dei giovani che (non è un caso) sono assidui (quando non compulsivi) fruitori dei “servizi della società dell’informazione” in questione, quali, ad es., i servizi di messaggistica istantanea, le piattaforme per la condivisione di materiali come fotografie o video o lo scambio di beni.

Premesso che “dati personali” sono elementi identificativi del soggetto (quali quelli anagrafici, l’indirizzo IP, la localizzazione, le preferenze rispetto ai siti visitati) e che possederli consente di orientare i gusti, indirizzando pubblicità mirata e alimentando così il mercato “finale”, non v’è ormai dubbio che essi rappresentino una merce preziosa e che quindi rispetto ad essa sia configurabile un (seppure peculiare e prodromico) “mercato dei dati”²⁷ dove diventano merce – e mezzo – di scambio; soprattutto considerando, aldilà di ogni

possibile lettura giuridica del fenomeno, il fatto che la loro cessione, che il consenso al “trattamento” implica, si presenta nella maggior parte dei casi come la *condicio sine qua non* per l’accesso al servizio stesso.

Ora, da un lato non si può omettere di considerare la facile aggirabilità “tecnica” dell’ostacolo dell’età minima, che solleva un ulteriore ordine di problemi applicativi, legati alla c.d. *age verification*, e legittime perplessità sulla reale efficacia della previsione. Proprio su questo si stanno concentrando, come meglio si vedrà, i tentativi di regolare tale verifica in modo da minimizzare l’accesso a contenuti inadatti.

Dall’altro, si può dubitare, invece, che il sedicenne e *a fortiori* il quattordicenne possano essere *in toto* equiparati in questo contesto, in ragione di tale “emancipazione digitale”, a qualsiasi altro soggetto “interessato” e che quindi le cautele che proprio con la verifica dell’età si vogliono prendere possano svanire una volta raggiunta la soglia del consenso digitale autonomo.

Se, poi, è lecito ancora dubitare (è tema assai noto e discusso) di un consenso autenticamente libero ed informato da parte degli stessi adulti, rispetto ai giovani(ssimi) ancor più facilmente questo elemento può esser percepito come “imposto”²⁸ invece che libero e più come ostacolo da rimuovere per soddisfare un desiderio che strumento di consapevolezza per entrare nel mondo digitale.

Soprascedendo qui sulla dibattuta questione della configurabilità e validità di un simile contratto che abbia nella cessione dei dati la controprestazione dei minori per il servizio, le implicazioni negoziali di detta cessione, che appaiono già intricate e oscure rispetto all’adulto, rispetto al minore rischiano di far perdere di vista l’obiettivo ultimo

25. «(...) Tale specifica protezione dovrebbe, in particolare, riguardare l’utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all’atto dell’utilizzo di servizi forniti direttamente a un minore (...).

26. «Tale diritto è in particolare rilevante se l’interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare tale tipo di dati personali, in particolare da internet. L’interessato dovrebbe poter esercitare tale diritto indipendentemente dal fatto che non sia più un minore». Per un commento CUFFARO–D’ORAZIO–RICCIUTO 2019, p. 353 ss. In argomento, di recente tornato in auge anche grazie all’avvento del GDPR, v. LIVI 2020; BELLOMIA 2019; in particolare sull’efficacia dell’ordine di rimozione, v. ASTONE 2020.

27. Come intende CUFFARO 2018, p. 35 s.

28. Cfr. BOZZI 2020, p. 266 ss.

della sua tutela²⁹, in questo specifico scenario; scenario che rappresenta, invece – paradossalmente – proprio uno di quelli in cui massimamente si svolge la personalità del minore e si articola quindi il suo sviluppo psico-fisico. È infatti evidente come l'uso dei social network in particolare, tra i servizi offerti, sia uno dei principali mezzi di socializzazione e di manifestazione del pensiero, concorrente quindi nella costruzione stessa dell'identità personale del giovane utente e responsabile della sua "esistenza digitale"³⁰.

Senza altro occorrerebbe che fosse spiegato soprattutto ai minori e in modo per loro comprensibile a che cosa esattamente acconsentono, immettendo i dati e autorizzandone il trattamento, nonché la ragione di scambio sottesa alla richiesta, che può arguirsi (solo), quando opera, dal meccanismo escludente, per cui senza autorizzazione l'accesso è negato. A tal proposito, la raccomandazione circa la semplicità e la chiarezza del linguaggio³¹ appare, tuttavia, a ben vedere, un presidio più apparente che reale, più di forma che di sostanza, inadeguato ad un'efficace e completa tutela.

In ciò si rileva, dunque, un'aporia del sistema: proprio in uno degli ambiti (lo spazio digitale) in cui il minore è più attivo ed esposto³² rischia di essere meno tutelato.

Una certa qual disinvoltura nel cedere i dati, infatti, già facilmente registrabile negli adulti – cui si può, tuttavia, rimproverare una scarsa ponderazione – tanto più la si riscontra mediamente nei minori, anche compiuti i 14 anni, proprio per l'inesperienza e la curiosità che li caratterizza e che giustificerebbe – per loro – un'analoga scarsa ponderazione.

Il minore, inoltre, quand'anche arrivasse a comprendere (grazie al linguaggio chiaro e sempre che ci si soffermi) le finalità per cui saranno trattati i suoi dati ben potrebbe non comprendere appieno o affatto la natura negoziale del gesto né i rischi della cessione propagabili nel tempo e nello spazio: coordinate entrambe potenzialmente infinite nel Web. E non si può omettere di considerare come sovente il linguaggio pur chiaro resti del tutto generico nell'indicare le finalità della raccolta, senza rappresentare né le possibili ulteriori finalità, né i possibili rischi connessi alla c.d. "profilazione"³³, né tanto meno la possibilità di incorrere o subire illeciti durante l'uso, profili che sicuramente non sono ricompresi nelle "informazioni e comunicazioni relative al trattamento che lo riguarda".

Se, come è stato osservato³⁴, con l'avvento della rivoluzione digitale siamo di fronte ad una nuova forma di identità, scaturente dalla circolazione di

29. Obiettivo che, rispetto all'informazione, di cui sia soggetto, oggetto o destinatario, per il minore è in ogni caso la tutela del suo armonico sviluppo fisico, psichico e morale: sul punto, per un maggiore approfondimento, sia consentito rinviare a AGOSTINELLI 2022.

30. «che talvolta assorbe o prevarica la loro esistenza fisica non virtuale»: così BIANCA 2019, p. 150. In argomento v. anche PERLINGIERI 2014.

31. Tradotta così nel nuovo art. 2 *quinquies*, c. 2, cod. privacy: «In relazione all'offerta diretta ai minori dei servizi di cui al comma 1, il titolare del trattamento redige con linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore, al fine di rendere significativo il consenso prestato da quest'ultimo, le informazioni e le comunicazioni relative al trattamento che lo riguarda».

32. Una dettagliata analisi del fenomeno è contenuta in AGCOM 2018. Il tema è oggetto di riflessioni plurime, tra le quali: RODOTÀ 2014, p. 13. In particolare sui rischi connessi alla navigazione in rete dei minori: ANDREOLA 2019; CAGGIANO 2018; PERLINGIERI 2016, p. 1327 ss.

33. Ovvero il trattamento automatizzato dei dati che rielabora particolari aspetti e abitudini della persona: v. considerando 71, ove peraltro si prevede che non dovrebbe «riguardare i minori». La raccomandazione non è stata poi riprodotta nell'articolato, per cui si discute se sia cogente; per un approfondimento si rinvia a PIERUCCI 2019, p. 448 s.; GARACI 2021, p. 817 ss. Sulla c.d. "filter bubble" coniata da Eli Pariser, che metaforicamente «evidenzia l'inglobamento della persona in una virtuale gabbia che raccoglie i dati, le preferenze, le scelte di prodotti o di servizi e che, attraverso un algoritmo, individua un preciso profilo» v. le riflessioni di BIANCA 2019-A, p. 39 ss.

34. ALPA 2017, per il quale «l'identità è diventata un concetto liquido. E il diritto alla identità un diritto connesso con una realtà fattuale fluttuante, dinamica, fluida, quasi inafferrabile. Di questa identità si è impossessata l'informatica, e l'ha piegata strumentalmente ai suoi usi patrimoniali».

simili dati, un'identità anch'essa digitale, esprimere il consenso in tale ambito significa più complessivamente gestire tale identità, ammettendo che i suoi estremi circolino.

La consapevolezza del duplice effetto della cessione – “divulgativo” e al contempo “costitutivo” della stessa identità digitale – spesso manca negli interessati maggiorenni: presumerla nei ragazzi, senza adeguate contromisure, rende ancora più illusoria l'autodeterminazione che il consenso dovrebbe rivelare e rende altresì illusoria l'attesa (o pretesa) da parte dell'art. 2-*quinqies*, cod. privacy di un consenso realmente “significativo”.

Quel grado di ponderazione in più allora sarebbe stato prudente, invece che estrometterli da ogni controllo, lasciarlo affidato e pretenderlo – per lo meno sotto forma di autorizzazione se non di sostituzione – dai genitori, posto che tale attività di assistenza – che infatti “resiste” fino al quattordicesimo anno – si iscrive pienamente come detto nella responsabilità e nel dovere di cura cui sono tenuti *ex artt.* 315 bis e 316 c.c.

I 14 anni rappresentano, dunque, una “maturità digitale” che è stata salutata, sull'onda di un certo “protagonismo minorile”, come una conquista evolutiva del minore, sempre più e prima slegata dall'autorizzazione genitoriale, e direttamente ammesso a gestire in modo autonomo i suoi diritti personali nonché per tale via, secondo alcuni, anche quelli patrimoniali immediatamente connessi³⁵.

Ma, a ben vedere, anche questa maturità digitale, non diversamente da quella ordinaria di cui all'art. 2 c.c., sconta, con i limiti propri di ogni criterio standard, l'automatismo di una data: il compimento del quattordicesimo anno, a prescindere dalla valutazione circa la cruciale “capacità di discernimento”³⁶, di cui non si fa menzione alcuna e che, invece, è di recente assunta a criterio-guida negli spazi di autonomia esistenziale previsti e che sola giustifica una simile anticipazione.

Diversamente dal passaggio alla maggiore età “ordinaria”, tuttavia, che presume il raggiungimento di un sufficiente grado di maturità idoneo alla generale cura dei propri interessi, la maturità digitale non è chiaro a quale tipo, o sottotipo, di maturità alluda.

Peraltro se è noto che lo sviluppo personale è il risultato dell'interazione di alcuni processi – biologici, cognitivi e socio-emotivi – e che nel *continuum* del processo di crescita possono distinguersi vari stadi evolutivi, è altrettanto noto che la maturità cognitiva non coincide necessariamente con quella emotiva, che consente di gestire le emozioni e prendere consapevolezza delle possibili conseguenze delle prozie azioni³⁷.

Proprio alla luce della particolare esposizione dei minori nel Web, l'esercizio della responsabilità genitoriale si articola in modo sempre più complesso e il dovere di educazione ed assistenza ma anche di guida e controllo non possono che contemplare in concreto anche le sempre nuove modalità di interazione dei figli (minori) con terzi attraverso l'uso di dispositivi digitali.

La semplice iscrizione ad un social network, ad esempio, per nulla “neutra”, produce, e pone, un problema di effettività e pienezza della protezione del (figlio) minore. Protezione che, in questa prospettiva, la spinta all'autonomia indotta dal consenso “anticipato” – pur in astratto condivisibile obiettivo di legislatore e interprete – rischia di compromettere o, in qualche misura, depotenziare.

Non si può non riconoscere, infatti, che il minore si trova spesso più *solo* che *autonomo* nel venire in contatto con una realtà virtuale della cui incidenza sulla sua sfera personale può non percepire la reale portata e che il guadagnato consenso, finalmente scevro da condizionamenti genitoriali, può però aprire ad una serie indefinita di altri condizionamenti da parte di terzi, sottratti questi ad ogni controllo³⁸.

35. Cfr. CAMARDI 2019, p. 125 ss.; SENIGAGLIA 2021, *passim*.

36. Sul punto, BOZZI 2020, p. 265 ss., che considera come presunto il discernimento del quattordicenne alla base del suo consenso. In tema, RUSCELLO 2011.

37. Sono, infatti, previste attualmente valutazioni specifiche di questi diversi aspetti del funzionamento mentale dell'individuo in età evolutiva: v. LINGIARDI-McWILLIAMS-SPERANZA 2020, p. 5 ss.

38. Tristemente noti i fenomeni, dilaganti specie nei ragazzini più fragili e condizionabili, che accettano tragiche “sfide” sui social, prestandosi ad atti di autolesionismo, fino all'estremo, o esibendo immagini intime di sé o di altri, condividendo contenuti su temi delicatissimi quali la depressione o i disturbi dell'alimentazione o il

3. I sistemi di *parental control*

Quale esplicazione di tali doveri genitoriali sono impiegabili meccanismi di *parental control*, strumenti di “filtro” nella navigazione in rete che consentono di supervisionare l’uso dei vari dispositivi – quali computer, tv, tablet e, soprattutto, smartphone – attraverso, ad esempio, l’autorizzazione o il blocco delle applicazioni, l’impostazione del tempo di riposo, il calcolo di quello trascorso, la verifica dei siti visitati, la geolocalizzazione del device e la possibilità di interdire l’accesso a determinate attività da parte del minore.

Detti sistemi di controllo non sono da ridurre solo ad una serie di accorgimenti tecnici per monitorare o co-gestire l’account del figlio ma vanno opportunamente considerati, come s’è detto, quale vera e propria “sottovoce” dell’educazione.

Proprio su tali meccanismi si è andata accentuando l’attenzione regolatoria negli ultimi provvedimenti normativi, volti evidentemente ad incentivarne il ricorso da parte dei genitori, specialmente allo scopo di inibire la visione di contenuti inadatti, in modo particolare quelli pornografici e violenti.

Infatti, mentre sul fronte eurounitario, è stato emanato il Reg. UE 2022/2065 (*Digital Services*

Act)³⁹ che ha, almeno in astratto, il merito di inscrivere tra i vari “rischi sistemici”, “reali o prevedibili”, che gli operatori di grandi dimensioni dovranno calcolare e comunicare (considerando 80-83), quelli relativi ai diritti del *minore*, approntando una serie di misure preventive, specie per l’accesso ai contenuti divulgati in rete⁴⁰, a livello domestico, con la delibera AGCOM 9/23/CONS del 25 gennaio 2023 sono state emanate, a seguito della consultazione pubblica con i principali operatori ed associazioni di categoria, le Linee guida in materia di sistemi di “protezione dei minori dal rischio del cyberspazio”. Tali Linee guida danno attuazione all’art. 7-*bis* del d.l. n. 28/2020, stabilendo che i contratti di fornitura nei servizi di comunicazione elettronica devono prevedere tra i servizi preattivati per le offerte dedicate ai minori proprio i sistemi di controllo parentale e anche quelli di filtro di contenuti inappropriati per i minori e di blocco di contenuti riservati ad un pubblico di età superiore agli anni diciotto, disattivabili solo su richiesta del consumatore maggiorenne o del genitore⁴¹. Gli operatori di telefonia, di reti televisive e di comunicazioni elettroniche devono altresì assicurare adeguate forme di pubblicità di tali servizi, onde assicurarne la massima diffusione.

cyberbullismo. Altrettanto noto il rischio di grooming, ossia l’adescamento on line, favorito proprio dalla facile creazione di un’identità fittizia anche da parte degli adulti che possono apparire minori.

39. In combinazione con il Reg. UE 2022/1925 sui mercati digitali (*Digital Markets Act*) all’interno di un unico disegno normativo volto a disciplinare, con modalità e mezzi diversi, l’offerta di prodotti e servizi all’interno del mercato digitale, coerentemente con la strategia per l’Europa digitale ed il Piano d’azione per la democrazia europea presentati nel 2020. Non si può non osservare che i minori sono parte e destinatari di tale mercato che li considera doppiamente interessanti: nell’immediato, quali consumatori attuali; in prospettiva, quali consumatori adulti, ormai avvezzi e ambientati. Posto che centrale in detto disegno normativo è l’obiettivo, a più riprese dichiarato (e di gran lunga preponderante), di «migliorare il funzionamento del mercato interno e garantire un ambiente online sicuro e trasparente» (considerando 41), non si fugge facilmente il sospetto che un «ambiente digitale sicuro» sia dunque (anche) funzionale a rendere il minore sempre prima autonomo perché divenga quanto prima un nuovo, indipendente ed attivo consumatore.

40. In particolare rispetto alla progettazione o all’uso, «anche mediante manipolazione, di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi, con ripercussioni negative, effettive o prevedibili, sulla tutela della salute pubblica e dei minori e gravi conseguenze negative per il benessere fisico e mentale della persona o per la violenza di genere». Per maggiori approfondimenti, si permetta il rinvio a AGOSTINELLI 2023-A, p. 412 ss.

41. Le principali categorie di contenuti a visione non libera sono state individuate in: contenuti per adulti, gioco d’azzardo, armi, violenza, odio e discriminazione, pratiche dannose per la salute, anonymizer, sette. Sul tema e sul funzionamento dei meccanismi di parental control e relative criticità, sia consentito rinviare ancora a AGOSTINELLI 2023-A, p. 397 ss.; AGOSTINELLI 2023, p. 179 ss. In argomento, v. anche BATTELLI 2021; D’AMBROGIO 2018.

Da ultimo, e sulla medesima scia, il d.l. 15 settembre 2023, n. 123 (“Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile nonché per la sicurezza dei minori in ambito digitale”, c.d. “decreto Caivano”), convertito con modificazioni dalla l. 13 novembre 2023, n. 159, dedica il Capo IV appunto alle “Disposizioni per la sicurezza dei minori in ambito digitale”.

In tale contesto – comprensivo anche della specifica tutela dei minori di anni diciotto rispetto all’accesso ai siti pornografici, espressamente vietato (art. 13-*bis*)⁴² – viene data una definizione normativa di “applicazioni di controllo parentale”, quali “elementi esterni a dispositivi di comunicazione elettronica, soluzioni a livello di rete o applicazioni o software per dispositivi di comunicazione elettronica, facilmente comprensibili e accessibili agli utenti, che consentano il controllo parentale”, quest’ultimo a sua volta definito come “possibilità di limitare e controllare, da parte dei genitori o di coloro che esercitano la responsabilità genitoriale, l’accesso ai contenuti e/o alla rete da parte dei minori, mediante la scelta degli spazi digitali e dei tempi di utilizzo” (art. 13).

Si prevede, in particolare, che, per garantire un ambiente digitale sicuro ai minori, i produttori assicurino, a monte dell’immissione sul mercato di dispositivi, che i sistemi operativi installati consentano l’utilizzo e includano la disponibilità di applicazioni di controllo parentale, da pubblicizzare appositamente e chiaramente nella confezione in fase di vendita; e, nelle more, che i fornitori di servizi di comunicazione elettronica assicurino, dal canto loro, senza costi aggiuntivi, la disponibilità di tali applicazioni già nell’ambito dei contratti di fornitura nei servizi di comunicazione elettronica

e provvedano ad avvisi mirati ai clienti già in essere per informarli della “possibilità ed importanza” di utilizzare simili applicazioni (art. 13, comma 7).

Viene così confermata la linea già tracciata di massima incentivazione dell’impiego di tali strumenti, oggetto poi di apposite campagne pubbliche di sensibilizzazione e di successive, specifiche verifiche annuali da parte dell’Agicom circa l’implementazione effettiva, insieme al rispetto anche dell’art. 13-*bis* (art. 14).

Illustrato così in sintesi il fronte normativo, non si può che condividere il perseguito scopo di favorire una cultura di maggiore attenzione e consapevolezza da parte dei genitori – troppo spesso i primi a sottovalutare i rischi di un uso precoce e scriteriato della rete – e di garantire un ricorso, quindi, massiccio a questi sistemi. Non si può, tuttavia, non rilevare che tali meccanismi protettivi, anche ove massicciamente adottati, proprio in ossequio della sopraggiunta “maturità digitale”, normalmente al quattordicesimo anno cessano di essere operativi; il che comporta lo sblocco simultaneo dei canali prima preclusi, delle funzionalità di “filtro” e di tutte le autorizzazioni genitoriali necessarie, sino a quel momento, per “accompagnare” e vigilare sulla navigazione del figlio. La disattivazione si può impedire, confermando la scelta iniziale di controllo, ma, a questo punto, non senza l’assenso del figlio che nel frattempo ha infatti maturato il diritto di manifestare direttamente, come s’è detto, il proprio “consenso digitale”.

I filtri disattivati, quindi, – salvo per i contenuti inadatti riservati agli ultradiciottenni, che devono restare inaccessibili, secondo l’obbligo gravante sugli operatori, incaricati della verifica dell’età – possono essere conservati o installati di nuovo ma solo con il consenso del figlio ultraquattordicenne,

42. La norma, introdotta in sede di conversione, impone ai fornitori di tale genere di contenuti di verificare la maggiore età degli utenti, al fine di evitare l’accesso ai minori di anni 18, in quanto questo «mina il rispetto della loro dignità e ne compromette il benessere fisico e mentale, costituendo un problema di salute pubblica». Si prevede altresì che l’Autorità per le garanzie nelle comunicazioni, entro sessanta giorni dalla data di entrata in vigore della legge di conversione e sentito il Garante per la protezione dei dati personali, individui le modalità per l’accertamento della maggiore età degli utenti, assicurando un livello di sicurezza adeguato al rischio e il rispetto della minimizzazione dei dati personali raccolti in ragione dello scopo: tale seguito è stato dato con la [delibera n. 61/24/cons](#) con cui si è avviata la consultazione pubblica per l’approvazione di un provvedimento che disciplini le modalità tecniche e di processo per l’accertamento della maggiore età degli utenti. L’elenco delle possibili modalità di verifica allo stato attuale, con le relative criticità, lo si può leggere nell’all. B a detta delibera. In argomento e per una rassegna delle soluzioni recentemente adottate anche negli altri ordinamenti nazionali si rinvia a CAPILLI 2024, p. 10.

che, in una distopica inversione di ruoli, dovrà a ciò autorizzare il proprio genitore e che in ogni caso e in ogni momento potrà successivamente interrompere la supervisione.

Dunque, se non sarà modificato questo assetto – il che pare assai difficile se resta ferma la “maturità digitale” a quattordici anni – dopo tale data i genitori si trovano ad essere deprivati, insieme al vaglio preventivo dei luoghi digitali frequentati dal figlio, di una “quota” di responsabilità genitoriale; si apre, per loro, una sorta di zona virtuale “franca” che sfugge alla conoscenza prima ancora che al controllo, dove la tutela dei minori e dai minori stessi si fa ulteriormente più complicata.

Tale sorta di “sottrazione” di competenza rende palese che quello dei minori in rete non è (e non crea solo) un problema di privacy, all’altare della quale viene improvvidamente sacrificato l’esercizio effettivo e compiuto della responsabilità genitoriale.

La (maggiore) sicurezza dell’ambiente digitale (ammesso che la si voglia realmente perseguire da parte dei decisori politici – nazionali e sovranazionali – e soprattutto degli operatori economici) non esonera i genitori dal controllo, nella consapevolezza che l’adempimento del compito è divenuto sempre più complesso ed arduo per i genitori, che non di rado sono meno abili dei figli nell’uso di detti strumenti. Questi ultimi, peraltro, se da un lato consentono la proiezione e la formazione stessa della personalità dei giovani utenti, dall’altro impongono, proprio per questo e per le potenzialità lesive connesse, un incremento di sorveglianza da parte degli adulti.

Né andrebbero sottovalutate, a tale proposito, le ricadute, in caso di condotte illecite poste in essere dal minore, anche sul piano di un’eventuale *culpa in vigilando* se non *in educando* (ex art. 2048 c.c.). Considerando che la nota prova liberatoria dalla relativa presunzione⁴³ è già di per sé ritenuta diabolica, calata nel contesto di un atto on line diviene praticamente impossibile, se persino l’addestramento diretto e partecipato al corretto uso del mezzo telematico viene inibito ai genitori in

nome di un’irretrattabile autonomia dei figli (appena) quattordicenni.

Ai genitori, che non sono messi in condizione di esercitare come prima la medesima vigilanza, vengono, per così dire, “spuntate” le armi proprio nel momento e nel luogo della massima esposizione al pericolo per i figli (sia di commettere sia di subire abusi) e proprio quando la necessità della specifica “educazione digitale” si fa più urgente.

Non è poi solo il possibile contatto con contenuti inadatti all’età ma è lo stesso meccanismo, ormai ampiamente noto, di cattura dell’attenzione che talune applicazioni adottano per prolungare il tempo di esposizione che è già di per sé potenzialmente nocivo. Questo tipo di effetto è scongiurabile attraverso un’adeguata guida ad un uso moderato del mezzo: il che è competenza esclusiva, si potrebbe dire, del genitore e non può essere delegato al mezzo medesimo.

Dunque l’idea stessa di un controllo genitoriale “a tempo” sconfessa quella di un esercizio pieno della responsabilità e modulato, caso per caso, sull’effettiva capacità di discernimento e maturità raggiunta dal figlio che non è uguale per ogni figlio e in ogni contesto familiare e in ogni tempo.

Da non sottovalutare anche un riflesso ulteriore: tale scelta normativa di un consenso anticipato non solo scoraggia i genitori, specie i meno solerti, dall’insistere nella sorveglianza rispetto ad un ambito in cui la legge stessa li esclude, ma tradisce un messaggio potenzialmente pericoloso per entrambi i soggetti della relazione: i genitori stessi che potrebbero, improvvidamente, percepire di essere “sollevati” in una certa misura dalla vigilanza, quando il figlio abbia conquistato l’autonomia digitale legale del consenso, che rende superfluo il loro coinvolgimento; i figli, cui viene consentito di estromettere i genitori dalle scelte sulla fruizione del Web e di resistere, a buon diritto, ad eventuali opposizioni di genitori pur solerti ma legalmente esautorati.

V’è poi da osservare che proprio perché il *parental control* è appunto una specifica forma di

43. «Di non aver potuto impedire il fatto», che, secondo l’interpretazione dominante, consiste nella prova (positiva) «di aver impartito al figlio una buona educazione e di aver esercitato su di lui una vigilanza adeguata, il tutto conforme alle condizioni sociali, familiari, all’età, al carattere, all’indole del minore»: v., *ex plurimis*, Cass., 20 ottobre 2005, n. 20322; Cass. 6 dicembre 2011, n. 26200. Emblematico il caso della responsabilità per la pubblicazione delle immagini intime di una minore ad opera di coetanei deciso da Trib. Sulmona, 9 aprile 2018, su cui THIENE 2018.

controllo e supervisione (cui per il resto i genitori sono tenuti), sarebbe comunque ben compatibile ammettere una manifestazione del consenso anticipata a quattordici anni e conservare in capo ai genitori il potere di valutare loro quale grado di supervisione impiegare nel caso concreto, in ragione di plurimi fattori legati alla singola persona del minore che l'attuale sistema invece automaticamente ed irragionevolmente azzerà, immaginando una categoria (gli ultraquattordicenni) del tutto indistinta ed omogenea, quale non è.

4. La tutela dei genitori e la tutela dai genitori: il fenomeno dello *sharenting*

Per un verso diametralmente opposto un corto circuito evidente tra esercizio della responsabilità genitoriale e “vigilanza digitale” si ha quando la presenza in rete del minore non solo non è impedita o sorvegliata ma è provocata dai genitori stessi.

Si fa riferimento al costume invalso tra questi ultimi di pubblicare sui profili dei propri social network fotografie e video della prole.

Il fenomeno è noto ormai con il termine *sharenting*, frutto della crasi tra *share* – condividere – e *parents* – genitori – che preoccupa, specie sul fronte della pediatria, per le variegate ripercussioni di una precoce esposizione on line⁴⁴.

La questione è approdata nelle aule di tribunale perlopiù nei casi di mancato consenso dell'altro genitore (quasi sempre ex partner) alla

divulgazione, e solitamente esita in pronunce, spesso cautelari, che ordinano la rimozione del materiale e ne inibiscono il nuovo inserimento in difetto di accordo genitoriale⁴⁵, talvolta applicando il rimedio ulteriore dell'*astreinte* ex art. 614-bis c.p.c., con la condanna al pagamento di una somma per ogni giorno di ritardo nella rimozione dell'immagine⁴⁶.

Tale contestabile condotta si ritiene integrare la violazione di plurime norme, nazionali, comunitarie ed internazionali⁴⁷ e si considera la diffusione quale interferenza nella vita privata del minore ritratto, pertanto “è necessario che il consenso alla pubblicazione di tali dati sia prestato dai genitori, in vece dei propri figli, concordemente fra loro e senza arrecare pregiudizio all'onore, al decoro e alla reputazione dell'immagine del minore (art. 97, l. n. 633 del 1941)”⁴⁸.

Dubbia, tuttavia, appare la linearità dell'argomentazione più ricorrente, indicativa, infatti, di una certa sovrapposizione di piani: se «il pregiudizio per il minore è insito nella diffusione della sua immagine sui social network sicché l'ordine di inibitoria e di rimozione va impartito immediatamente»⁴⁹, il consenso di entrambi (e non già di uno solo) alla pubblicazione non potrebbe valere e bastare a scongiurarlo.

Non è, infatti, solo e tanto una questione di abuso del diritto di immagine altrui né di formale

44. Come riportato dalla Documentazione per l'esame di Progetti di legge *In materia di minori e Internet, con riferimento particolare all'accesso alle piattaforme e all'uso dell'immagine dei minori* AA.C. 1217, 1771, 1800 e 1863 (v. *supra*, nota 20) uno studio pubblicato sul Journal of Pediatrics, ogni anno i genitori condividono on line una media di 300 fotografie riguardanti i propri figli e, prima del loro quinto compleanno, ne hanno già condivise quasi 1.000; in Europa, in particolare il 73% dei bambini ha una qualche presenza on line prima dei 2 anni. In argomento, cfr. FOGLIA 2022; ANDREOLA 2021, p. 857 ss.; SCIA 2020; CAMARDI 2019; THIENE 2017; THIENE 2012.

45. V., ad. es., Trib. Trani, 30 agosto 2021, con nota di ZANOVELLO 2022; Trib. Mantova, 19 settembre 2017, in “Famiglia e diritto”, 2018, p. 380 ss. Significativo che Trib. Chieti, 21 luglio 2020, in “Dirittifondamentali.it”, sulla questione della pubblicazione di foto del minore, sollevata nel giudizio di divorzio da ciascun genitore verso l'altro, abbia “prescritto a entrambi i genitori di astenersi da dette pubblicazioni in assenza di consenso esplicito dell'interessato (ormai entrato nel diciassettesimo anno d'età)”.

46. V. ad. es., Trib. Roma, 23 dicembre 2017, con nota di NITTI 2018; Trib. Trani, ord. 30 agosto 2021, cit.

47. Art. 10 c.c.; artt. 1 e 16 della Convenzione di New York, per cui «Nessun fanciullo sarà oggetto di interferenze arbitrarie nella sua vita privata, nella sua famiglia, nel suo domicilio o nella sua corrispondenza e neppure di affronti illegali al suo onore e alla sua reputazione» e «Il fanciullo ha diritto alla protezione della legge contro tali interferenze o tali affronti»; art. 8 Reg. UE 679/2016.

48. Trib. Trani, 30 agosto 2021, cit.

49. Trib. Mantova, 19 settembre 2017, cit.; Trib. Roma, 23 dicembre 2017, cit.

autorizzazione del soggetto ritrattato (art. 10 c.c., artt. 96 e 97 l. dir. autore).

Che detto consenso congiunto (a differenza di quando è il soggetto ritrattato adulto ad autorizzare per sé) integri una forma di esercizio della responsabilità genitoriale ex art. 316 c.c. è lecito dubitare, posto che non si tratta di un agire nell'interesse del figlio ma, semmai, in quello (futile e) egoistico di rendere pubblici e visibili momenti di vita personale (addirittura prenatale) e situazioni familiari le più disparate (dal primo giorno di scuola, ai compleanni, a progressi in qualche attività).

È semmai da chiedersi se, al contrario, non rappresenti piuttosto una violazione del dovere di protezione connesso alla responsabilità.

Il rispetto del riserbo dovuto dal genitore, infatti, si iscrive sempre nel medesimo alveo della responsabilità genitoriale, posto che, a differenza di qualsiasi altro adulto, il ruolo qui ricoperto qualifica la relazione in modo specifico e comporta obblighi specifici, più estesi e pregnanti del generale e generico dovere di astensione predicabile per i diritti della personalità riferiti anche ai minori.

Dunque la violazione della riservatezza del minore in tali casi (anche qui da valutare singolarmente per ordine di gravità) integra contestualmente una violazione del *munus* genitoriale.

E anche qui si è di fronte ad un evidente – e urgente – problema culturale⁵⁰, probabilmente non ancora adeguatamente percepito né indagato, ma che ha ricadute giuridiche certe, perché l'adempimento dei doveri di cura è una questione giuridica (oltretutto senza dubbio morale e sociale) e il relativo deficit è già un inadempimento.

Proprio per quanto detto a proposito del contenuto della responsabilità, la difesa dei diritti dei figli è naturalmente da pretendersi anche contro i genitori stessi.

Da ultimo, anche la Corte di Cassazione⁵¹, in una vicenda che riguardava l'uso dell'immagine di un bambino per fini pubblicitari in esecuzione di un contratto di sponsorizzazione stipulato da un

genitore, ha ribadito quanto ormai già affermato reiteratamente: il consenso deve essere espresso da entrambi i genitori; ed ha aggiunto che, configurandosi l'immagine quale elemento «altamente caratterizzante l'identità dell'individuo, unico e originale, come tale riconoscibile» l'uso di per sé illegittimo può essere altresì fonte di danno e meritevole di risarcimento «a condizione che sia accertata l'effettività e la serietà della lesione», «senza che la mancanza di indicazioni relative al nome e alle generalità del minore o dei suoi genitori valga ad escluderne il pregiudizio»⁵².

Anche in questo caso, per la verità, la lesione dell'immagine del bambino – largamente diffusa nel Web – è sfondo di un conflitto di coppia dove la condizione del figlio appare come uno dei più pregnanti argomenti di scontro genitoriale.

Scontro che di per sé sconfigge un corretto esercizio della responsabilità genitoriale e senza il quale è invero ben difficile che l'abuso dell'immagine del minore e la diffusione della pratica dello *sharenting* venga effettivamente contrastata.

Che la reale esigenza di tutela del minore sia, in simili vicende, il vero fulcro del contenzioso è, infatti, plausibile dubitare.

Il focus della pronuncia, ricca di riferimenti a fonti e giurisprudenza sovranazionali in tema di immagine e privacy, anche del minore, resta, infatti, sul consenso e non travalica quel problema di illiceità “procedurale” per andare al cuore della tutela del minore e della questione: non quella di essere esposto sulla base di un consenso bigenitoriale ma non essere esposto affatto. Che è quanto potrebbe preferire, se in grado di esprimersi in tale senso, il protagonista stesso⁵³.

Qui si ingarbuglia la matassa: il diritto al riserbo dei figli minori che i genitori non solo possono ma devono difendere nei confronti dei terzi loro per primi lo devono rispettare⁵⁴, considerati i rischi che una precoce esposizione anche ingenua porta con sé (su tutti, il reimpiego di terzi e la rielaborazione delle immagini in contesti pedopornografici).

50. Sull'inadeguatezza e l'insufficienza del diritto, attestata anche dalla giurisprudenza in tema, «ad affrontare un problema di tipo culturale che concerne anche l'educazione all'uso della rete», v. FOGLIA 2022, p. 3558.

51. Cass., 21 agosto 2024, n. 23018.

52. Con questo argomento, invece, nelle sedi di merito era stata rigettata la domanda risarcitoria.

53. Cfr. MOROTTI 2023. Ma v. ancora Trib. Chieti, 21 luglio 2020, nota 45.

54. CAMARDI 2019, p. 129.

E di più si ingarbuglia quando proprio il diritto al riserbo i genitori devono poter, per tutt'altro verso, contravvenire ove l'ingerenza nella privata dei figli rappresenti l'esercizio della dovuta vigilanza, strumentale alla protezione del minore stesso o dal minore stesso ove il pericolo (si pensi al cyberbullo) provenga – e non sia subito – da lui⁵⁵.

Recentemente la Francia si è mossa nell'ottica di tutelare i figli proprio rispetto alle stesse condotte genitoriali di diffusione delle immagini, intervenendo sul codice civile.

L'art. 371-1 cod. civ. come modificato dalla loi n. 2024-120 del 19.2.2024 «*visant à garantir le respect du droit à l'image des enfants*», dopo aver esordito affermando che «*L'autorité parentale est un ensemble de droits et de devoirs ayant pour finalité l'intérêt de l'enfant*», prosegue «*Elle appartient aux parents jusqu'à la majorité ou l'émancipation de l'enfant pour le protéger dans sa sécurité, sa santé, sa vie privée et sa moralité, pour assurer son éducation et permettre son développement, dans le respect dû à sa personne*».

La "vita privata" ha fatto dunque ufficialmente ingresso (questa la portata innovativa della norma che prima non la contemplava) nel catalogo dei beni oggetto di doverosa tutela da parte dei genitori.

Ancora, l'art. 371-2 cod. civ. viene significativamente modificato dalla medesima loi n. 2024-120 con l'introduzione della disposizione specifica sul diritto all'immagine: «*Les parents protègent en commun le droit à l'image de leur enfant mineur, dans le respect du droit à la vie privée mentionné à l'article 9. Les parents associent l'enfant à l'exercice de son droit à l'image, selon son âge et son degré de maturité*».

Inoltre, l'art. 377 cod. civ., anch'esso novellato, consente al giudice di delegare a terzi l'esercizio del diritto all'immagine quando «*la diffusion de l'image de l'enfant par ses parents porte gravement atteinte à la dignité ou à l'intégrité morale de celui-ci*».

Anche in Italia si sta pensando a delle forme di intervento normativo.

Ora, l'idea di normare è già di per sé una dichiarazione di fallimento della genitorialità, troppo

frequentemente inquinata da un certo narcisismo che induce a coinvolgere (e travolgere) anche la propria prole nella rappresentazione di sé.

I progetti depositati di recente⁵⁶ mirano a ridurre il fenomeno esigendo (come già emerso in giurisprudenza) il consenso di entrambi i genitori e l'obbligo di coinvolgere il minore "nell'esercizio dei suoi diritti di immagine, secondo la sua età e il suo grado di maturità" o impongono la comunicazione all'Autorità garante nelle comunicazioni (AGCOM) in caso di "diffusione delle immagini di un minore di anni quattordici tramite un servizio di piattaforma per la condivisione di video, in cui il minore stesso è il soggetto principale oppure partecipa al contenuto diffuso dal genitore".

A parte la patente difficoltà di un'ineffettiva applicazione (e quindi efficacia) della norma, in difetto di un conflitto genitoriale che possa far emergere la violazione, non si vede come il semplice consenso genitoriale duplice possa prevenire la sovraesposizione e fornire reale tutela.

Ove questo ricorra, il figlio finisce per essere esposto (come normalmente accade) su iniziativa (e sui social network) di entrambi i genitori. In tal senso, le proposte allo studio paiono non cogliere nel segno.

Il diverso, ma connesso, fenomeno dei c.d. *baby influencer*, cui pure i medesimi disegni si dedicano, è per certi aspetti addirittura più inquietante: qui l'esposizione on line costituisce addirittura fonte di lucro e sul punto i progetti di legge⁵⁷, lungi dall'inibire una simile attività, mirano ad (almeno) disciplinare il fenomeno a vantaggio (economico) del minore.

Se forse è sbrigativo e superficiale affermare che tali cennate condotte siano segno di mancata o inadeguata cura filiale, certamente non si può non osservare che nessuno, prima dell'era digitale, avrebbe mai pensato di patentare un minore e di metterlo alla guida di un'auto, neppure con il consenso dei genitori.

Che sia la legge a dover intervenire è, oltretutto inutile, desolante, atteso che dovrebbe essere superfluo un intervento volto, in un ambito così

55. *Ivi*, p. 132 ss. ricorda come la questione sia duplice: l'ingerenza deve essere giustificata, quindi legittima, quanto «all'an del potere/dovere di interferire con la riservatezza»; poi si pone il problema del quantum e/o del quomodo il genitore ossa spingersi nella conoscenza o nella ricerca di dati personali sulla vita del figlio.

56. AA.C. 1771, 1800.

57. AA.C. 1217, 1771, 1800 e 1863.

delicato e cruciale come il rapporto genitori-figli, a ribadire e specificare quanto già contenuto nella sostanza di quel complessivo – e complesso – dovere di cura sulla persona del minore in formazione che si condensa nella responsabilità genitoriale *ex artt. 315-bis e 316 c.c.*

Ancora più desolante immaginare, come la casistica giurisprudenziale suggerisce, che di un eventuale potenziamento del diritto all'immagine del minore possa avvalersi in modo strumentale un genitore contro l'altro, a detrimento di questi piuttosto che a beneficio del figlio.

5. Conclusioni: nuovi confini per la responsabilità genitoriale

Lo spazio dove si muovono bambini e ragazzi si è ampliato e i relativi confini sono nuovi perché si è di molto allargata la loro possibilità e libertà di movimento.

Proprio l'elasticità della nozione di responsabilità genitoriale consente di ricomprenderci addirittura la (apparente) ingerenza nella sfera privata del figlio ove tale ingerenza rappresenti l'esercizio del doveroso controllo delle attività on line: queste non solo possono rivelarsi (alla luce proprio di detto controllo) pericolose e nocive per il figlio stesso che le subisca ma anche pericolose o nocive per altri, ove sia il figlio ad infliggerle.

Il diritto alla riservatezza del minore⁵⁸, sicuramente funzionale alla costruzione dell'identità personale, dovrebbe arretrare nel caso il genitore abbia ragione di credere che sia (o possa venire) compromessa la dignità, il diritto all'onore o alla

reputazione o, addirittura, alla salute del minore stesso o di terzi che con lui siano entrati in contatto.

Proprio il dilagante (e faticosamente contrastato)⁵⁹ fenomeno del cyberbullismo – con i drammatici esiti che la cronaca troppo spesso racconta – conferma che la supervisione degli adulti (i genitori, ragionevolmente prima di ogni altra figura di riferimento) è necessaria sia per fornire uno scudo alle vittime sia per disarmare i (giovani) “aguzzini” digitali.

Impossibile, o meglio pericoloso, escludere un vaglio sulla necessità di tale supervisione, da farsi caso per caso, a seconda delle circostanze del caso concreto, delle caratteristiche (età compresa) del singolo figlio e del contesto di riferimento singolarmente considerabile.

Una volta che i genitori abbiano insegnato ai figli ad attraversare la strada da soli, occorre insegnare loro anche ad attraversare la rete da soli, in modo da gradualmente avvezzarli al mondo, sia reale che virtuale, entrambi diversamente insidiosi.

Il controllo che rientra nelle fasi intermedie della crescita non è fine a se stesso, né espressione di un prepotere sovraordinato che vuole conservarsi integro fino al limite massimo della maggiore età; non va letto neppure come un sacrificio necessario – ma da ridurre al minimo – della libera autodeterminazione del figlio.

È, piuttosto, funzionale alla vigilanza quale espressione, a sua volta, dell'accudimento e dell'educazione, che nell'instillare il rispetto di se stessi e degli altri realizza uno dei suoi più irrinunciabili obiettivi.

Riferimenti bibliografici

AGCOM (2018), *Libro bianco “Media e Minori”*, 2018

B. AGOSTINELLI (2024), *Diritti e doveri del figlio*, in F. Galgano, G. De Nova (a cura di), “Commentario del Codice civile Scialoja-Branca”, Zanichelli, 2024

B. AGOSTINELLI (2023), “*Emancipazione digitale*” e tutela dei minori tra responsabilità genitoriale e regolamentazione eurounitaria, in R. Torino, S. Zorzetto (a cura di), “La trasformazione digitale in Europa. Diritti e principi”, Giappichelli, 2023

B. AGOSTINELLI (2023-A), *Minori in rete: l'illusione del consenso e l'equivoco della privacy*, in “*Famiglia*”, 2023, n. 3

58. Cfr. in argomento MARCHIO 1998, p. 569 ss.; THIENE 2017; CAMARDI 2018, p. 838 ss.

59. Dalla l. 29 maggio 2017, n. 71, come modificata recentemente dalla l. 17 maggio 2024, n. 70.

- B. AGOSTINELLI (2022), *Informazione e minori: una lettura integrata per una tutela uniforme*, in “Jus civile”, 2022, n. 2
- B. AGOSTINELLI (2021), *L'educazione della prole tra antiche prerogative genitoriali e nuovo interesse del minore*, in “Rivista di diritto civile”, 2021, n. 1
- E. AL MUREDEN (2014), *Dalla potestà alla responsabilità genitoriale*, in “Giurisprudenza italiana”, 2014, n. 5
- G. ALPA (2017), *L'identità digitale e la tutela della persona. Spunti di riflessione*, in “Contratto e impresa”, 2017, n. 3
- E. ANDREOLA (2021), *Misure cautelari a tutela dei minori nei social network*, in “Famiglia e diritto”, 2021, n. 8-9
- E. ANDREOLA (2019), *Minori e incapaci in Internet*, Edizioni Scientifiche Italiane, 2019
- M. ASTONE (2020), *Il diritto all'oblio on line alla prova dei limiti territoriali*, in “Europa e diritto privato”, 2020, n. 1
- E. BATTELLI (2021), *Minori e social network: cyberbullismo e limiti della parental responsibility*, in “Corriere giuridico”, 2021, n. 10
- V. BELLOMIA (2019), *Diritto all'oblio e società dell'informazione*, Cedam, 2019
- C.M. BIANCA (2023), *Diritto civile - 2.1, La famiglia*, 7^a ed. a cura di M. Bianca e P. Sirena, Giuffrè, 2023
- M. BIANCA (2019), *Il minore e i nuovi media*, in R. Senigaglia (a cura di), “Autodeterminazione e minore età. Itinerari di diritto minorile”, Pacini Giuridica, 2019
- M. BIANCA (2019-A), *La filter bubble e il problema dell'identità digitale*, in “MediaLaws”, 2019, n. 2
- C.M. BIANCA (2015), *Note introduttive*, in Id. (a cura di), “La riforma della filiazione”, Cedam, 2015
- L. BOZZI (2020), *I dati del minore tra protezione e circolazione: per una lettura non retorica del fenomeno*, in “Europa e diritto privato”, 2020, n. 1
- F.D. BUSNELLI (2016), *Il diritto della famiglia di fronte al problema della difficile integrazione delle fonti*, in “Rivista di diritto civile”, 2016, n. 6
- I. CAGGIANO (2018), *Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del regolamento UE 2016/679, tra diritto e tecno-regolazione*, in “Familia”, 2018, n. 1
- C. CAMARDI (2019), *Minore e privacy nel contesto delle relazioni familiari*, in R. Senigaglia (a cura di), “Autodeterminazione e minore età. Itinerari di diritto minorile”, Pacini Giuridica, 2019
- C. CAMARDI (2018), *Relazione di filiazione e privacy. Brevi note sull'autodeterminazione del minore*, in “Jus civile”, 2018, n. 6
- G. CAPILLI (2024), *Minori in rete tra consenso e verifica dell'età. Analisi comparata e proposte di adeguamento al GDPR*, in “Medialaws”, 2024, n. 1
- A.G. CIANCI (2014), *Dal concetto di potestà al concetto di responsabilità genitoriale: norme di raccordo*, in M. Bianca (a cura di), “Filiazione. Commento al decreto attuativo. Le novità introdotte dal d.lgs. 28 dicembre 2013, n. 154”, Giuffrè, 2014
- V. CUFFARO (2018), *Il diritto europeo sulla protezione dei dati e la sua applicazione in Italia: spunti per un bilancio*, in A. Mantelero, D. Poletti (a cura di), “Regolare la tecnologia. Il Reg. Ue 2016-679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna”, Pisa University Press, 2018
- V. CUFFARO (2018-A), *Quel che resta di un codice: il D.Lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al regolamento sulla protezione dei dati*, in “Il Corriere giuridico”, 2018, n. 10

- V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di) (2019), *I dati personali nel diritto europeo*, Giappichelli, 2019
- F. D'AMBROGIO (2018), Parental control: *accorgimenti tecnici per escludere la fruizione da parte dei minori di contenuti classificati a visione non libera*, in "Familia", 2018, n. 1
- G. DE CRISTOFARO (2014), *Dalla potestà alla responsabilità genitoriale: profili problematici di una innovazione discutibile*, in "Le Nuove leggi civili commentate", 2014, n. 4
- M. DOGLIOTTI (2019), *Capacità, incapacità, diritti degli incapaci. Le misure di protezione*, in "Trattato di diritto civile e commerciale già diretto da A. Cicu e F. Messineo L. Mengoni e continuato da Piero Schlesinger", Giuffrè, 2019
- M. FOGLIA (2022), *Sharenting e riservatezza del minore in rete*, in "Actualidad Jurídica Iberoamericana", 2022, n. 16 bis
- I. GARACI (2021), *Il "superiore interesse del minore" nel quadro di uno sviluppo sostenibile dell'ambiente digitale*, in "Le Nuove leggi civili commentate", 2021, n. 4
- F. GIARDINA (1977), *I rapporti personali tra genitori e figli alla luce del nuovo diritto di famiglia*, in "Rivista trimestrale di diritto e procedura civile", 1977, n. 4
- F. GIARDINA (1990), voce *Minore - I) Diritto civile*, in "Enciclopedia giuridica Treccani", vol. XXII, 1990
- A. GORASSINI (2014), *La responsabilità genitoriale come contenuto della potestà*, in M. Bianca (a cura di), "Filiazione. Commento al decreto attuativo. Le novità introdotte dal d.lgs. 28 dicembre 2013, n. 154", Giuffrè, 2014
- A. GORASSINI (2012), *Lo stato unico di genitore*, in U. Salanitro (a cura di), "Il sistema del diritto di famiglia dopo la stagione delle riforme", Pacini Giuridica, 2012
- L. LENTI (2021), *Diritto della famiglia*, Giuffrè, 2021
- L. LINGIARDI, N. MCWILLIAMS, A.M. SPERANZA (a cura di) (2020), *Manuale diagnostico psicodinamico PDM-2 0/18. Infanzia e adolescenza*, Raffaello Cortina Editore, 2020
- M.A. LIVI (2020), *Quale diritto all'oblio?*, Jovene, 2020
- E. LUCCHINI GUASTALLA (2019), *Privacy e data protection: principi generali*, in E. Tosi (a cura di), "Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy", Giuffrè, 2019
- A.M. MARCHIO (1998), *Profili del diritto alla riservatezza dei minori di età*, in "Studi in onore di Pietro Rescigno", vol. 2, Giuffrè, 1998
- L. MENGONI (1982), *La tutela giuridica della vita materiale nelle varie età dell'uomo*, in "Rivista trimestrale di diritto e procedura civile", 1982, n. 4
- V. MONTARULI (2019), *La protezione dei dati personali e il minore*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019
- T. MONTECCHIARI (2006), *La potestà dei genitori*, Giuffrè, 2006
- E. MOROTTI (2023), *Il dissenso del minore alla pubblicazione delle proprie immagini in rete*, in "Familia. it", 2023
- M. NITTI (2018), *La pubblicazione di foto di minori sui social network tra tutela della riservatezza e individuazione dei confini della responsabilità genitoriale*, in "Famiglia e diritto", 2018, n. 4
- A. PALAZZO (2013), *La filiazione*, in "Trattato Cicu-Messineo", 2ª ed., Giuffrè, 2013
- S. PATTI, L. ROSSI CARLEO (a cura di) (2021), *L'esercizio della responsabilità genitoriale*, in F. Galgano, G. De Nova (a cura di), "Commentario del Codice civile Scialoja-Branca", Zanichelli, 2021

- C. PERLINGIERI (2016), *La tutela dei minori di età nei social networks*, in “Rassegna di diritto civile”, 2016, n. 4
- C. PERLINGIERI (2014), *Profili civilistici dei social networks*, Edizioni Scientifiche Italiane, 2014
- A. PIERUCCI (2019), *Elaborazione dei dati e profilazione delle persone*, in V. Cuffaro, R. D’Orazio, V. Ricciuto (a cura di), “I dati personali nel diritto europeo”, Giappichelli, 2019
- G. RECINTO (2016), *Le genitorialità. Dai genitori ai figli e ritorno*, Edizioni Scientifiche Italiane, 2016
- S. RODOTÀ (2014), *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, 2014
- F. RUSCELLO (2015), *Autonomia dei genitori, responsabilità genitoriale e intervento pubblico*, in “La Nuova Giurisprudenza Civile Commentata”, 2015, n. 12
- F. RUSCELLO (2012), *Potestà dei genitori versus responsabilità*, in “Comparazione e diritto civile”, 2012
- F. RUSCELLO (2011), *Minore età e capacità di discernimento: quando i concetti assurgono a “supernorme”*, in “Famiglia e diritto”, 2011, n. 4
- F. RUSCELLO (2006), *La potestà dei genitori. Rapporti personali*, Giuffrè, 2006
- U. SALANITRO (2014), *La riforma della disciplina della filiazione dopo l’esercizio della delega (I parte)*, in “Corriere giuridico”, 2014, n. 4
- P. SCHLESINGER (2014), *Il d.lgs. n. 154 del 2013 completa la riforma della filiazione*, in “Famiglia e diritto”, 2014, n. 5
- F. SCIA (2020), *Diritti dei minori e responsabilità dei genitori nell’era digitale*, Edizioni Scientifiche Italiane, 2020
- R. SENIGAGLIA (2021), *Minore età e contratto. Contributo alla teoria della capacità*, Giappichelli, 2021
- G. SPOTO (2016), *Disciplina del consenso e tutela del minore*, in S. Sica, V. Antonio, G.M. Riccio (a cura di), “La nuova disciplina europea della privacy”, Cedam, 2016
- A. THIENE (2018), *Ragazzi perduti online: illeciti dei minori e responsabilità dei genitori*, in “La Nuova Giurisprudenza Civile Commentata”, 2018, n. 11
- A. THIENE (2017), *Riservatezza e autodeterminazione del minore nelle scelte esistenziali*, in “Famiglia e diritto”, 2017, n. 2
- A. THIENE (2012), *L’inconsistente tutela dei minori nel mondo virtuale*, in “Studium iuris”, 2012, n. 5
- B. VOLPI (2017), *Genitori digitali. Crescere i propri figli nell’era di Internet*, il Mulino, 2017
- F. ZANOVELLO (2022), *Foto dei figli sui social e tutela cautelare e d’urgenza*, in “La Nuova Giurisprudenza Civile Commentata”, 2022, n. 1



LORENZO MARIA LUCARELLI TONINI

Strumenti di *age verification* alla luce del contributo del Garante privacy e dell'AGCOM: il rischio di obsolescenza tecnologica e conoscitiva

L'articolo intende analizzare il complesso tema della tutela dei soggetti minori di età nell'ambito delle attività che essi svolgono online. In particolare, partendo dal presupposto per cui la presenza dei minori in rete è una realtà consolidata, verrà affrontato il tema della verifica dell'età del minore, c.d. "age verification", alla luce del contesto normativo di riferimento, al fine di individuare un possibile bilanciamento tra la necessità di garantire l'accesso ai c.d. "servizi della società dell'informazione" e la necessità di apprestare una "tutela rafforzata" in virtù dei potenziali rischi presenti nella Rete. Si procederà, nello specifico, ad analizzare i principali provvedimenti emanati dall'Autorità garante per la protezione dei dati personali e dall'Autorità per le garanzie nelle comunicazioni, al fine di verificare l'efficacia dei mezzi disponibili in tema di "age verification".

Minori – Online – Age verification – Privacy – Piattaforme

Age verification tools in the light of the contribution of the Data Protection Authority and AGCOM: the risk of technological and cognitive obsolescence

This paper intends to analyse the complex theme of the protection of minors in the context of the activities they carry out online. In particular, starting from the assumption that the presence of minors online is a consolidated reality, the theme of the verification of the age of the minor will be addressed in the light of the regulatory context of reference, in order to identify a possible balance between the need to guarantee access to the so-called "services of the information society" and the need to provide a "strengthened protection" in virtue of the potential risks present on the Net. Specifically, the main measures issued by the Authority for the protection of personal data and by the Authority for the guarantees in communications will be analysed in order to verify the effectiveness of the means available on the subject of age verification.

Minors – Online – Age verification – Privacy – Platforms

L'Autore è dottorando di ricerca in Discipline giuridiche, curriculum di Diritto pubblico, presso l'Università degli Studi Roma Tre

Questo contributo fa parte della sezione monografica *Minori e Internet* a cura di Carlo Colapietro e Antonio Iannuzzi

SOMMARIO: 1. Introduzione. – 2. *Age verification* tra complessità fenomenica e inquadramento normativo. – 2.1. *I provvedimenti dell'Autorità garante per la protezione dei dati personali*. – 2.2. *I provvedimenti dell'Autorità per le garanzie nelle comunicazioni*. – 3. Brevi osservazioni conclusive.

1. Introduzione

Il pervadere dell'uso delle tecnologie digitali in tutti i settori della società moderna pone oggi gli attori coinvolti di fronte a nuove sfide: nella specie, il giurista è chiamato a vagliarne le conseguenze¹ in termini di bilanciamento tra utilità, quindi benefici, e tutela delle situazioni giuridiche soggettive rilevanti. In questa sede, si fa particolare riferimento alla tutela del minore di età, da considerarsi sotto il binario schema costituzionale di «soggetto di diritti» o «soggetto di bisogni»². Occorre quindi verificare sia le potenziali conseguenze positive che l'uso delle tecnologie può avere sulla crescita e sull'inclusione del minore nella società, quindi sull'autodeterminazione delle «modalità di costruzione della propria sfera privata»³, sia le eventuali conseguenze dannose anche alla luce dell'adeguatezza, o meno, degli strumenti messi a disposizione dalla tecnica e dalla legge. Si consideri, infatti, che «dal momento della nascita sino al raggiungimento della maggiore età, l'individuo vive quindi in una peculiare condizione, caratterizzata dalla costante tensione tra categorie giuridiche e realtà fattuale», tale per cui «l'equilibrio tra queste due condizioni [...] si traduce in un forte condizionamento della vita del minore, non solo da un punto di vista

strettamente giuridico, quindi della tutela della sua dimensione costituzionale di titolare di diritti fondamentali⁴, ma anche, e soprattutto, in considerazione delle prospettive di vita nella collettività»⁵.

Ormai è infatti necessario consentire l'accesso dei minori a tecnologie digitali, che siano però effettivamente positive per lo sviluppo degli stessi; tuttavia, considerato che il minore può essere a ragione definito un vero e proprio consumatore di beni e servizi digitali, in particolare «il più debole tra i consumatori», in quanto «mentre il consumatore è occasionalmente il soggetto debole del contratto, il minore lo è per *status*»⁶, è al contempo necessario individuarne l'età al fine consentirne, parametrarne o addirittura inibirne l'uso delle tecnologie digitali, nonché attivare l'insieme di tutele rafforzate previste dalla normativa esistente, *in primis* in materia di protezione dei dati personali. Dunque, anche se per il minore è oggi particolarmente familiare l'uso delle nuove tecnologie, tale da renderlo spesso anche più abile rispetto ai maggiori di età, non è negabile come lo stesso sconti però, di base, una minore consapevolezza dei rischi, dei propri diritti e del «valore» dei propri dati⁷, tale per cui «non si tratta solo di riconoscere al minore la libertà di «decidere» in merito alla

1. Approfondisce il tema MARTONI 2021; MARTONI 2020.

2. DI COSTANZO 2023.

3. RODOTÀ 1995, p. 101 ss.

4. In tema v. STANZIONE-SCIANCELEPORE 2006.

5. GIARDA-LIOTTA-RINDI 2022, p. 185.

6. ANDREOLA 2019, p. 12.

7. Condividono tale ricostruzione OROFINO 2018; CAGGIANO 2018; SCIA 2018, p. 21 ss.; NADDEO 2018; BRAVO 2017, p. 167 ss.; SPOTO 2016, p. 111 ss.

sua sfera privata, ma di metterlo nelle condizioni – soggettive e oggettive – di assumere decisioni consapevoli⁸.

Si veda, inoltre, come se da una parte la normativa, complessivamente considerata, preveda chiaramente l'esigenza di apprestare una "tutela rafforzata" per i minori che utilizzano le tecnologie digitali, sia allo stesso tempo difficile garantirne la reale applicazione, sia per la molteplicità e la complessità delle diverse tipologie di strumenti a ciò destinati, sia per la capacità dei minori, quali nativi digitali, di eluderne spesso l'applicazione. Inoltre, si consideri una forte attrazione dei minori verso la realtà online, dovuta all'apparente gratuità di molti dei servizi digitali. Si consideri anche il ruolo non sempre costruttivamente determinante rivestito dai genitori o da chi ne faccia le veci, seppure ormai al posto del «tradizionale modello autoritario e gerarchico del rapporto genitore figlio», sono stati ormai preferiti «modelli educativi improntati al dialogo ed alla crescente attenzione all'autodeterminazione dei minori», che oggi si arricchiscono di «una ulteriore dimensione educativa che riguarda il comportamento in rete, rischi e opportunità»⁹.

Il contesto di riferimento è, infine, reso ulteriormente complesso da una parte dalla subdola pervasività delle tecnologie cui hanno accesso i minori, tale da non consentire sovente una valutazione reale del loro impatto e da cui deriva, dunque, una duplice esigenza di protezione da rinvenirsi sia in riferimento alle tecnologie stesse, sia ai contenuti tramite queste veicolati.

2. Age verification tra complessità fenomenica e inquadramento normativo

Per addivenire ad un quadro esaustivo degli strumenti destinati alla verifica dell'età del minore che accede alle tecnologie digitali, svolgendo quindi quella che viene definita attività di "age verification" e verificarne dunque i requisiti, è tuttavia necessario partire da una breve ricostruzione dei termini normativamente previsti, potendosi solo in seguito

giungere all'analisi degli strumenti effettivamente esistenti, con particolare attenzione ai più recenti provvedimenti emanati dall'Autorità garante per la protezione dei dati personali e dall'Autorità per le garanzie nelle comunicazioni.

Si veda anzitutto come manchi ad oggi una definizione condivisa dell'attività di "verificazione dell'età", potendosi ricondurre a tale concetto l'insieme degli strumenti e dei procedimenti volti a verificare l'età di un soggetto, in specie per qualificarlo come minore o meno e che possono consistere, in via generale, nella verifica posta in essere dal fornitore della tecnologia o del servizio digitale, nella dichiarazione stessa della persona o, infine, in azioni di verifica poste in essere da terzi incaricati. Quanto all'ambito di indagine, invece, questo è costituito principalmente dal contesto di Internet, anche se non esclusivamente, inteso come ambiente e strumento nel quale e tramite il quale molte delle tecnologie o dei contenuti oggetto di indagine vengono veicolati. In riferimento, invece, al concetto di "minore", si veda come questo sia da intendersi con riguardo al raggiungimento, o meglio al mancato raggiungimento di una certa soglia di età, al di sotto della quale, per una presunta carenza di piena capacità di agire, è inibita la possibilità di porre in essere in autonomia la maggior parte delle azioni che abbiano conseguenze giuridiche sulla propria o altrui sfera giuridica, pur residuando specifiche ed eccezionali limitate capacità di contrarre¹⁰.

Il fenomeno, inoltre, deve essere ulteriormente considerato osservando come «la casistica si distingue maggiormente tra ipotesi in cui il genitore accede ai contenuti pubblicati liberamente dal figlio, ed ipotesi in cui diffonde egli stesso immagini o informazioni riguardanti i figli minori sui social network, senza il loro consenso ovvero all'insaputa o contro la volontà dell'altro genitore»¹¹, finanche in ipotesi in cui i genitori sono invece totalmente all'oscuro della presenza online del minore.

Calando quanto anticipato sin qui all'interno di previsioni di carattere normativo o para-normativo,

8. IRTI 2019.

9. Così MARCELLO 2022, p. 1311.

10. Il tema della capacità d'agire dei minori è oggetto di ampia trattazione in dottrina: senza presunzione di completezza si rimanda a ALPA 2004; CAPILLI 2012; CINQUE 2007; PANUCCIO DATTOLA 2009; SENIGAGLIA 2020.

11. STELLA 2022, p. 1433.

è possibile anzitutto porre le basi della necessità di garantire una tutela rafforzata del minore rispetto all'uso delle tecnologie, anche attraverso l'uso di strumenti di "age verification", nella "Convenzione delle Nazioni Unite sui Diritti del Fanciullo"¹² che, nel riconoscere come "bambino" il minore degli anni diciotto, cristallizza il principio fondamentale del "*best interest of the child*"¹³. Per quanto qui di principale interesse, il Comitato sui Diritti del Fanciullo, cui è demandato il controllo sull'applicazione della Convenzione e di cui si segnala principalmente il "Commento generale n. 25 (2021) sui diritti dei minorenni in relazione all'ambiente digitale", ha avuto modo di esplicitare che l'accesso dei minori alle tecnologie debba essere ponderato e consapevole, attraverso l'adozione di «appropriati meccanismi operativi che supportino i minorenni, i genitori e altri adulti di riferimento nell'ottenere l'accesso alle forme di protezione applicabili», tra cui «sistemi di verifica dell'età per impedire ai minorenni di accedere a prodotti e servizi il cui possesso o utilizzo risultino illegali per loro».

Occorre però precisare come un preminente ruolo in tema di tutela dei minori e nuove tecnologie sia da rinvenire nel Reg. Ue 679/2016, meglio conosciuto come GDPR, il quale con un impatto diretto sulle attività di trattamento dei dati personali connesse all'uso delle moderne tecnologie, impone una «protezione rafforzata» del minore, in termini di informazioni, espressione del consenso, verifica dell'età e misure di sicurezza. Si veda,

tuttavia, come seppure la normativa sia comune ed omogenea, proprio il settore della tutela dei minori online e in particolare del trattamento dei dati personali dei minori, sia stato oggetto di adattamenti, nel limite di quanto consentito, da parte dei singoli ordinamenti nazionali¹⁴.

Prendendo le mosse dalla considerazione per cui i minori sono «meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate, nonché dei loro diritti in relazione al trattamento dei dati personali»¹⁵, tali da essere destinatari di una specifica protezione in quanto «vulnerabili»¹⁶, il GDPR, riconoscendo nel consenso una delle principali basi giuridiche a legittimazione delle attività di trattamento dei dati personali, dispone all'art. 8 che, qualora la finalità sia quella dell'offerta di «servizi della società dell'informazione»¹⁷, tra cui principalmente rientrano i servizi web a cui i minori quotidianamente hanno accesso, essi, in qualità di «interessati», possano autodeterminarsi nel caso in cui abbiano compiuto almeno il sedicesimo anno di età. Rispetto a tale disposizione, così come previsto, «gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni»: sul punto, l'ordinamento italiano, seguendo la scelta intrapresa da altri ordinamenti europei, ha novellato il d.lgs. 196/2003 (c.d. "Codice Privacy") raggiungendo una soluzione di «compromesso»¹⁸ e prevedendo, all'art. 2-*quiquies* che «il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei

12. La "Convenzione delle Nazioni Unite sui Diritti del Fanciullo", formalmente conosciuta come "Convenzione delle Nazioni Unite sui Diritti dell'Infanzia e dell'Adolescenza", è stata adottata dall'Assemblea Generale delle Nazioni Unite il 20 novembre 1989; essa costituisce, in quanto trattato internazionale, la principale fonte a livello mondiale per il riconoscimento e la tutela dei diritti civili, politici, economici, sociali e culturali dei bambini.

13. In tema, senza pretesa di completezza, v. LAMARQUE 2023; BIANCA 2021; PADELLETTI 2018; LAMARQUE 2016.

14. Per quanto riguarda la comparazione delle scelte normative di adeguamento al GDPR intraprese dai diversi Stati membri, si rimanda a CAPILLI 2024.

15. Considerando n. 38 del GDPR.

16. Considerando n. 75 GDPR.

17. La definizione di "servizio della società dell'informazione" è dettata dalla direttiva (UE) 2015/1535, all'art. 1, co. 1, lett. b), il quale fa riferimento a «qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi».

18. Secondo CAPILLI 2024: «si rivela chiaramente, tuttavia, che la norma che riguarda i minorenni è frutto di un compromesso, considerato la previsione di un unico limite di età, che non diversifica in relazione ai servizi né tantomeno valorizza il ruolo dei minori nella società moderna, potrebbe incidere in modo sproporzionato sui loro diritti e sulle loro opportunità».

propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione»¹⁹. Ciò è stato dettato dall'esigenza di garantire al minore una maggiore libertà di azione, in un contesto, quale la società digitale, ove l'uso delle tecnologie digitali, in specie i servizi della società dell'informazione, è da considerarsi fondamentale per il suo sviluppo. Tuttavia, si veda come tale previsione non abbia modificato l'ordinario assetto normativo previsto in tema di capacità d'agire, sistematicamente regolato in via generale dal Codice Civile. Quel che qui risulta fondamentale è considerare come il legislatore europeo abbia posto a carico di chi tratta i dati personali del minore al fine di fornirgli l'accesso al servizio, un chiaro obbligo di verifica della validità del consenso prestato nei termini di legge previsti dall'art. 4 del GDPR, compreso dell'età di chi lo esprime e in considerazione degli strumenti disponibili. Ciò, determina che nel caso dei "servizi della società dell'informazione" questi, qualora siano diretti anche ai minori, dovranno essere accessibili tramite adeguati sistemi di verifica dell'età, al quale faccia seguito la predisposizione di misure e contenuti differenziati in ragione dell'età stessa degli utenti. Ne deriva che il consenso, quando prestabile da parte del minore, dovrà essere non solo "libero", quindi frutto di un'autonoma determinazione ma anche, a tal fine, "informato": sul punto, l'art. 12 del GDPR prevede infatti che le informazioni relative al trattamento dei dati personali dei minori debbano essere fornite in forma «concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni

destinate specificamente ai minori». Il titolare del trattamento, dunque, ha la responsabilità di scegliere e calibrare i mezzi e un linguaggio adeguato, mettendo il campo «ogni ragionevole sforzo per verificare che l'utente abbia raggiunto l'età del consenso digitale», adottando misure «proporzionate alla natura e ai rischi delle attività di trattamento»²⁰ e, nel caso in cui l'interessato affermi il raggiungimento dell'età del consenso digitale, persiste un ulteriore obbligo di effettuare controlli, definibili "di secondo grado", «appropriati per verificare la veridicità della dichiarazione», non potendosi diversamente considerare sufficiente, in qualunque caso, la mera dichiarazione del minore²¹ stesso. Non si può, tuttavia, non menzionare il fatto che sovente, invece, sia da parte del minore sia da parte dei titolari del trattamento, al netto degli obblighi e dei diritti citati, vi sia una scarsa attenzione in merito, tale da rischiare di far degradare, se non addirittura annullare, l'efficacia e l'adeguatezza²² dello strumento del "consenso digitale".

È proprio mediante la lettura di tali informazioni sul trattamento dei dati personali che, oltre ad essere edotti delle modalità di trattamento dei dati e quindi della loro adeguatezza rispetto al minore destinatario, è possibile comprendere se il servizio sia, in ragione del suo oggetto, un servizio che è possibile considerare come positivo per lo sviluppo e la crescita del minore e quindi adeguato.

Nulla dice il GDPR, invece, per quanto riguarda il caso in cui il minore non abbia raggiunto l'età del "consenso digitale" e siano quindi i genitori ad esprimerlo: in questo caso, si applicheranno le regole generali di espressione del consenso²³,

19. Tuttavia, l'originale previsione, precedente alle modifiche introdotte dal d.lgs. 10 agosto 2018, n. 101, individuava nei tredici anni l'età minima: la modifica è stata dettata anche dalla necessità di uniformare tale previsione con altre norme che individuano il riferimento dei 14 anni, ad esempio la legge n. 184 del 1983 sull'adozione o la legge n. 71 del 2017 sul cyberbullismo.

20. A riguardo, v. EUROPEAN DATA PROTECTION BOARD 2020.

21. Sottolinea SCORZA 2023 che «il famoso GDPR dice espressamente che sotto i sedici anni – quattordici in Italia – un bambino non è in grado di prestare al fornitore di un servizio digitale il consenso a trattare i suoi dati. Ma, naturalmente, se quel bambino dichiara di essere più grande e il gestore gli crede, il problema è risolto o, almeno, online, si fa spesso finta che sia così».

22. A riguardo, si veda come infatti non sia unanimemente condivisa la scelta del legislatore di prevedere nel "consenso digitale" un valido strumento di legittimazione del trattamento dei dati del minore. Sul punto, v. BATTELLI 2022, pp. 543-562.

23. Non di secondo rilievo è a riguardo stabilire quando i genitori possano esprimersi singolarmente oppure vi sia la necessità di un consenso congiunto: non avendo il legislatore europeo affermato alcunché, dovrà quindi

avendo cura di osservare, tuttavia, come ciò determini implicitamente il trattamento dei dati di ulteriori soggetti, i genitori, con una finalità strumentale al principale trattamento dei dati dei minori; a riguardo, l'EDPB ha raccomandato un «approccio proporzionato» al raggiungimento della finalità di trattamento, teso a riconoscere e fare esprimere il consenso genitoriale attraverso il trattamento di una «quantità limitata di informazioni», in base al tipo di servizio offerto e alla tipologia di trattamento.

Da quanto detto, emerge subito una delle questioni principali rispetto al tema della verifica dell'età dei minori e dell'espressione del consenso digitale, anche quando prestato dai genitori: tale attività, che costituisce un adempimento di legge, comporta essa stessa la necessità di trattare ulteriori dati personali, ove tale trattamento risulta strumentale a garantire la legittimità del trattamento principale. Da qui, la necessità di rendere conforme anche tale attività di trattamento, che necessita quindi di essere parametrata, rispetto agli strumenti e ai principi in tema di *data protection*, al trattamento principale, tale per cui trattamenti complessi e rischiosi abbisognerebbero di una verifica dell'età maggiormente analitica e rigorosa, mentre trattamenti di carattere comune e meno rischiosi possono essere legittimati da una verifica dell'età meno pervasiva ma comunque efficace.

Si veda, dunque, che gli strumenti utilizzati per verificare l'età dei minori o, in alternativa, per acquisire il consenso del genitore, possono essere molteplici e generalmente catalogabili nei sistemi basati sulla «dichiarazione dell'età», i sistemi basati sulla «verifica dell'età» e quelli basati sulla «stima dell'età»: tutti comportano un diverso livello di «profondità» del trattamento dei dati personali. Inoltre, tali sistemi sono oggi sempre più digitalizzati, quindi caratterizzati da tecnologie differenti,

rappresentandone la più avanzata espressione i sistemi basati sull'utilizzo dell'intelligenza artificiale: a riguardo, si ricordi che la materia è stata di recente regolata dal c.d. «*Ai Act*»²⁴, il quale, differenziando i diversi modelli di intelligenza artificiale in base al rischio, prevede espressamente anche una tutela specifica in tema di minori di età.

Inoltre, a completamento del quadro regolatorio sin qui delineato, si veda come anche il «Digital Service Act» (DSA)²⁵, nell'intenzione di garantire maggiore sicurezza nel mercato della fornitura dei beni e dei servizi digitali, dedichi particolare attenzione proprio ai minori, prevedendo in capo ai c.d. «prestatori di servizi online» l'obbligo di progettare interfacce chiare e adatte agli utenti minori di età, stabilendo quali contenuti gli siano accessibili e progettando sin dall'inizio servizi adeguati.

Svolge una funzione particolarmente importante proprio la verifica dell'età del minore, preliminare alla valutazione dell'adeguatezza dei servizi offerti: sul punto, il «DSA» prevede tra gli strumenti di «attenuazione dei rischi» previsti dall'art. 15, «l'adozione di misure mirate per tutelare i diritti dei minori, compresi strumenti di verifica dell'età e di controllo parentale».

Al netto, dunque, dell'esistenza di specifici obblighi di verifica dell'età del minore, non sempre sufficientemente declinati quanto invece, anche in applicazione della disciplina prevista dal GDPR, lasciati alla scelta del titolare del trattamento e al netto delle diverse esperienze nazionali, sono stati sviluppati e adottati nel tempo molteplici e diversificati strumenti.

In Italia, un ruolo maggiormente decisivo è stato svolto dall'Autorità garante per la protezione dei dati personali e dall'Autorità per le garanzie nelle comunicazioni, entrambe coinvolte, sotto i diversi profili di competenza, nel complesso processo di individuazione di strumenti validi a consentire

farsi riferimento alla normativa e agli orientamenti nazionali, essendo quindi rilevante comprendere se si tratti di un atto di ordinaria amministrazione o di straordinaria amministrazione. Si consideri come il consenso del genitore riguardi un diritto, quello alla protezione dei dati personali, ritenuto «fondamentale» e che, quindi, richiederebbe in principio l'espressione del consenso di entrambi i genitori.

24. Regolamento europeo del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (legge sull'intelligenza artificiale), approvato e pubblicato sulla Gazzetta Ufficiale dell'Unione europea il 12 luglio 2024.

25. Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).

un corretto bilanciamento tra verifica dell'età del minore, la protezione dei dati personali e l'accesso alle tecnologie digitali.

Si procederà dunque ora ad analizzare i principali provvedimenti in materia, anticipandosi già ora come molti degli interventi siano stati sino ad oggi tendenzialmente volti a dettare principi generali: ciò, si ritiene sia dovuto sia alla principale disciplina di riferimento, quindi il GDPR, il quale rimette a chi tratta i dati la scelta dell'individuazione degli specifici strumenti e delle tecnologie volte alla verifica dell'età, sia, ad una caratteristica fondamentale del tema di cui si occupa, ossia il fatto che le tecnologie sono di per sé obsolete e regolarle analiticamente rischia di non essere efficace; inoltre, tali tecnologie risultano doppiamente obsolete in virtù del fatto che i beneficiari della regolazione sono i minori, ossia nativi digitali, come tali spesso in grado di eludere, se non anticipare, i sistemi così come progettati e regolati.

2.1. I provvedimenti dell'Autorità garante per la protezione dei dati personali

Prendendo le mosse dagli interventi ritenuti maggiormente rilevanti dell'Autorità garante per la protezione dei dati personali, già con il *vademecum* "Minori e nuove tecnologie. Consigli ai «Grandi» per un utilizzo sicuro da parte dei «Piccoli», pubblicato nel febbraio 2021, il Garante privacy ha posto l'attenzione sui pericoli che la rete nasconde e sulla necessità di garantire una tutela rafforzata per i minori: il Garante si è in tale occasione rivolto sia ai titolari del trattamento (quali i fornitori dei servizi online), sia ai genitori, recuperando, rafforzando ed aggiornando il ruolo e gli obblighi in tema di responsabilità genitoriale previsto dalla legge. A tal fine, ad esempio, i genitori vengono chiamati a calibrare i dispositivi regolandoli secondo le impostazioni più sicure, utilizzando i filtri e le restrizioni relative alla privacy, anche attraverso appositi strumenti di *parental control* e inibendo l'accesso a determinati servizi e piattaforme. Se da una parte, quindi, i rischi e le misure individuate dal Garante riguardano direttamente i minori in

qualità di utenti digitali, dall'altra, tuttavia, rilevanti sono i richiami e i moniti diretti anche ai genitori, i quali non solo devono, nell'esercizio della propria potestà genitoriale, vigilare sul corretto utilizzo delle nuove tecnologie da parte dei minori, ma anche evitare di porli direttamente, spesso inconsapevolmente, in condizioni di rischio, ad esempio pubblicando online immagini (c.d. "*sharenting*")²⁶ che potrebbero essere utilizzate per fini illeciti.

Con un noto provvedimento²⁷ relativo ad un social network assiduamente utilizzato dai minori, il Garante ha invece disposto la misura della limitazione dell'attività di trattamento dei dati relativi ai minori, di fatto inibendone l'accesso alla piattaforma web, in considerazione della «non assoluta certezza dell'età e, conseguentemente, del rispetto delle disposizioni collegate al requisito anagrafico». In particolare, il Garante non aveva ritenuto le misure adottate per la verifica dell'età adeguate e sicure, in quanto la mera indicazione dell'età, per di più ad opera dello stesso utente, è considerata un metodo facilmente aggirabile e non efficace. Inoltre, ritenendo che molti degli utenti della piattaforma fossero proprio minori, il Garante aveva individuato anche la carenza di una idonea informativa specificamente dedicata agli stessi, quindi chiara e semplice, che consentisse l'espressione di un valido ed informato consenso.

Con un provvedimento più recente²⁸, invece, il Garante, intervenuto sul tema della pubblicità personalizzata e della corretta base giuridica, ha avuto modo di fissare alcuni principi fondamentali relativi alla verifica dell'età. Nell'evidenziare come il presupposto legittimante dell'individuazione della corretta base giuridica debba essere preventivamente considerato quale «presupposto sostanziale del trattamento dei dati» e sia da rinvenirsi in una delle condizioni previste dal GDPR sin dall'inizio dell'attività di trattamento, il Garante ha anzitutto rilevato come diretta conseguenza sia il fatto che questa non possa essere modificata e piegata sulla base delle necessità e della discrezionalità del titolare del trattamento. Ogni modifica deve essere effettiva e riflettersi, ad esempio, in una modifica

26. A riguardo v. CACCIOPPO 2024.

27. Autorità garante per la protezione dei dati personali, [Provvedimento del 22 gennaio 2021](#) – Registro dei provvedimenti n. 20 del 22 gennaio 2021.

28. Autorità garante per la protezione dei dati personali, [Provvedimento del 7 luglio 2022](#) – Registro dei provvedimenti n. 248 del 7 luglio 2022.

dell'attività di trattamento. Strettamente legato a quanto affermato è proprio il tema dell'individuazione dell'età del minore al fine di stabilire la corretta base giuridica utilizzabile nei suoi confronti: viene quindi posta come ago della bilancia l'acquisizione del "consenso digitale", superati i 14 anni di età. Necessario, dunque, secondo le conclusioni del Garante è predisporre strumenti e misure di sicurezza specificamente finalizzate a consentire la corretta individuazione dell'età del minore, affinché l'interessato non sia destinatario di trattamenti che ad egli non potrebbero essere rivolti, oppure sia destinatario di trattamenti basati su una condizione legittimante carente o non applicabile.

Ancora, con un altro recente provvedimento²⁹, relativo ad una nota applicazione di intelligenza artificiale, il Garante aveva evidenziato che l'applicazione, pur indirizzata anche ai soggetti minori di età ma espressamente vietata ai minori di 13 anni, risultava carente degli strumenti e dei filtri atti a verificare l'effettiva età degli utenti e quindi inibirne l'uso ai soggetti esclusi oppure verificarne l'età per esprimere un valido consenso. Inoltre, risultando assente un sistema di verifica dell'età dell'utente, l'applicazione appariva anche priva di un sistema di blocco automatico qualora lo stesso avesse dichiarato di avere un'età non idonea. Alcuna informazione, infatti, era fornita nella *privacy policy*, con la conseguente impossibilità di comprendere quali e come i dati fossero trattati e in costanza di quale base giuridica.

Rimanendo in tema di intelligenza artificiale³⁰, seppure nell'ambito di un diverso provvedimento, il Garante ha avuto modo di rilevare come, pur essendo formalmente il servizio digitale riservato agli utenti maggiori degli anni 13, in realtà la piattaforma non avesse implementato alcun sistema effettivo di individuazione dell'età, esponendo i minori di anni 13 agli stessi output, in alcuni casi inappropriati, destinati ai soggetti legittimati ad

utilizzare la piattaforma. Ne è seguito un successivo provvedimento³¹, con il quale il Garante si è pronunciato richiedendo ai fini della piena riattivazione del servizio la predisposizione «in sede di primo accesso, di un *age gate* che escluda, sulla base dell'età dichiarata, gli utenti minorenni», chiedendo al titolare del trattamento di sottoporre all'Autorità «un piano per l'adozione di strumenti di *age verification* idoneo a escludere l'accesso al servizio agli utenti infra-tredicenni e a quelli minorenni, in assenza di un'espressa manifestazione di volontà da parte di chi esercita sugli stessi la responsabilità genitoriale», senza tuttavia indicare gli elementi essenziali da rispettare per l'attuazione.

Ad oggi, dunque, pur risultando chiari gli obblighi che i titolari del trattamento, in via generale, sono tenuti a rispettare nel trattare i dati dei minori nell'ambito della fornitura di servizi online, non sono tuttavia ancora state emanate dal Garante privacy vere e proprie istruzioni relative agli aspetti chiave e alle caratteristiche tecniche che i titolari del trattamento devono implementare nello sviluppo e nell'uso di sistemi di *age verification*, rimanendo ciò demandato, nello spirito della normativa in questione – il GDPR –, ai titolari, in base alle finalità perseguite nonché ai mezzi a disposizione.

2.2. I provvedimenti dell'Autorità per le garanzie nelle comunicazioni

Come si è avuto modo di anticipare, il tema della verifica dell'età dei minori che accedono ai servizi della società dell'informazione, coinvolgendo i settori delle comunicazioni elettroniche, dei media e delle piattaforme online, incrocia le competenze³² anche dell'Autorità per le garanzie nelle comunicazioni, la quale, in sinergia con il Garante privacy ha avuto modo di seguire e monitorare attivamente i processi tecnologici che riguardano l'utilizzo da parte dei minori delle tecnologie digitali. Oltre ai

29. Autorità garante per la protezione dei dati personali, [Provvedimento del 2 febbraio 2023](#) – Registro dei provvedimenti n. 39 del 2 febbraio 2023.

30. Autorità Garante per la protezione dei dati personali, [Provvedimento del 30 marzo 2023](#) – Registro dei provvedimenti n. 112 del 30 marzo 2023.

31. Autorità garante per la protezione dei dati personali, [Provvedimento dell'11 aprile 2023](#) – Registro dei provvedimenti n. 114 dell'11 aprile 2023.

32. Più dettagliatamente si rinvia all'art. 1, co. 6, della l. 31 luglio 1997, n. 249 che ha istituito l'Autorità e ne ha specificato le competenze. Ulteriori prerogative sono state successivamente previste ad opera del legislatore.

numerosi atti di indirizzo anzitempo emanati³³, l'Autorità è intervenuta in maniera maggiormente pragmatica adottando apposite linee guida³⁴ in tema di "parental control", specificando a carico degli *Internet service providers* (ISP) un obbligo di implementazione e messa a disposizione dei genitori, adeguatamente informati dell'esistenza³⁵, di strumenti, di cui le linee guida specificano i requisiti minimi, che permettano di limitare o bloccare l'accesso a determinate attività da parte di un minore, impedendo l'accesso, tramite qualunque applicazione, a contenuti inappropriati in ragione dell'età e specificando che gli strumenti di *parental control* ("SCP") «sono inclusi e attivati nelle offerte dedicate ai minori» e «resi disponibili come attivabili da parte del titolare del contratto». Quel che preme evidenziare in questa sede è come i soggetti individuati da AGCOM debbano porre in essere tale adempimento gratuitamente e come requisito strutturale del servizio stesso, senza poter condizionare l'accesso al servizio principale al pagamento di somme accessorie per i servizi di *parental control* messi a disposizione o l'accettazione stessa di tali servizi.

Di recente pubblicazione è invece il provvedimento³⁶, posto in consultazione pubblica

dall'AGCOM con delibera n. 61/24/CONS al fine di addivenire ad un documento condiviso circa gli strumenti attuali e successivamente approvato³⁷, con il quale l'Autorità ha delineato le caratteristiche che i sistemi di verifica dell'età devono implementare, proponendone uno specifico modello. Si anticipa anzitutto come appaia trasparire dalle intenzioni dell'AGCOM la volontà di addivenire alla proposta di sistemi di controllo dell'età di ampio respiro, per la quale l'Autorità ha quindi preso in considerazione le diverse normative ed esperienze nazionali, intendendo «valutare, nell'ambito della consultazione pubblica ..., se il sistema di verifica dell'età delineato nel documento posto in consultazione mediante l'indicazione di requisiti generali e di indicatori di performance sia efficace, idoneo e funzionale a trovare applicazione, ai sensi del contesto normativo da ultimo richiamato, anche con riferimento ad ulteriori tipologie di contenuti che potrebbero nuocere allo sviluppo fisico, mentale o morale dei minori».

Prendendo le mosse dalla considerazione dell'insufficienza ed inadeguatezza degli strumenti di verifica dell'età sino ad oggi resi disponibili³⁸, con il citato provvedimento l'Autorità ha inteso perseguire un approccio definito dichiaratamente

33. Si veda ad esempio AGCOM 2014 e AGCOM 2018.

34. AGCOM, Linee guida per l'attuazione dell'articolo 7-bis del decreto-legge 30 aprile 2020, n. 28 in materia di "sistemi di protezione dei minori dai rischi del cyberspazio", approvate con la delibera n. 9/23/CONS del 25 gennaio 2023, recante "Adozione delle linee guida finalizzate all'attuazione dell'articolo 7-bis del decreto-legge 30 aprile 2020, n. 28 in materia di «sistemi di protezione dei minori dai rischi del cyberspazio»".

35. A riguardo, le suddette linee guida specificano che «gli ISP pubblicano sui propri siti web guide chiare ed esaustive per l'utilizzo dei SCP ed offrono assistenza gratuita per l'attivazione, la disattivazione e la configurazione dei SCP attraverso call center con operatore umano ove selezionato dal consumatore secondo la vigente regolamentazione».

36. Il provvedimento segue quanto previsto dal d.l. 15 settembre 2023, n. 123, recante "Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori in ambito digitale" (cd. decreto Caivano), così come convertito, con modificazioni, dalla legge 13 novembre 2023, n. 159 e, in particolare, dall'art. 13-bis in cui viene demandato ad AGCOM il compito di emanare, sentito il Garante per la protezione dei dati personali (il quale si è espresso favorevolmente con il provvedimento n. 88 dell'8 febbraio 2024), un provvedimento che individui le modalità tecniche che i gestori di siti web e i fornitori delle piattaforme di condivisione video, che diffondono in Italia immagini e video a carattere pornografico, sono tenuti ad adottare per l'accertamento della maggiore età degli utenti, assicurando un livello di protezione adeguato al rischio e il rispetto della minimizzazione dei dati personali raccolti in ragione dello scopo.

37. Si fa riferimento alla Delibera 61/24/CONS del 25 marzo 2024 relativa ad uno schema di regolamento che disciplina le modalità tecniche e di processo per l'accertamento della maggiore età degli utenti, approvato da AGCOM in data 25 settembre 2024 e attualmente sottoposto al vaglio della Commissione europea.

38. Vengono individuati ad esempio i sistemi basati sull'autodichiarazione, sull'uso della carta di credito, sui sistemi di biometria, sull'analisi del comportamento online, sulla verifica dell'identità online (e sui sistemi di identità

«neutrale», quindi che «lasci ai soggetti tenuti alla realizzazione dei processi di *age assurance* una ragionevole libertà di valutazione e scelta, stabilendo tuttavia i principi e i requisiti che devono essere soddisfatti dai sistemi messi in campo».

Pur abbracciando un simile approccio, si segnala sin da ora come l'AGCOM, a differenza del Garante privacy, maggiormente incentrato a dare conto dell'applicazione dei principi generali in tema di *data protection*, abbia inteso scendere maggiormente nel dettaglio ed individuare le caratteristiche che i sistemi in parola debbono rispettare. Viene ad esempio indicata la "proporzionalità" del sistema, da intendersi come non invasività della sfera giuridica rispetto al fine che si propone di raggiungere; la conformità dello strumento rispetto alla normativa in tema di protezione dei dati personali; il preferenziale coinvolgimento di soggetti terzi, indipendenti ed attendibili, evitando che la verifica dell'età sia svolta direttamente dal fornitore del servizio digitale; la sicurezza dei sistemi, in grado dunque di fronteggiare eventuali attacchi informatici o tentativi di elusione. Un sistema che risponde a queste caratteristiche deve inoltre, secondo quanto precisato dall'AGCOM, essere «preciso» ed «efficace», contenendo dunque la possibilità di errore della valutazione dell'età, anche laddove vengano utilizzati sistemi di intelligenza artificiale adeguatamente allenati ma che, allo stesso tempo, dovrebbero risultare neutrale o indipendente dal dispositivo di accesso o dal sistema operativo utilizzato dall'utente; requisito necessario per garantirne l'efficacia è inoltre da considerarsi la facilità d'uso del sistema, dovendo quindi trattarsi di strumenti basati sulla capacità dei minori, non dovendo però allo stesso tempo costituire un ostacolo rispetto all'accesso ad Internet, nei casi consentiti, adottando quindi logiche di inclusività e non discriminazione. Infine, i sistemi di *age verification* devono essere trasparenti, tali per cui gli utenti devono essere messi a conoscenza del loro utilizzo e del loro funzionamento, dovendosi allo stesso tempo fornire ai soggetti coinvolti (minori, educatori, genitori...) la necessaria formazione per utilizzare correttamente tali strumenti e, in caso di funzionamento errato,

dovrebbero essere implementati adeguati sistemi di reclamo.

Dopo averne delineato, ad ampio spettro, le caratteristiche generali, con il citato provvedimento l'AGCOM, passando in rassegna i progetti maggiormente significativi sviluppati anche in ambito europeo, ha proposto un specifico modello di procedimento volto alla verifica dell'età, ponendolo appunto alla consultazione pubblica. Sulla base dei principi delineati, il sistema di verifica dell'età deve basarsi su un soggetto terzo, che fornisca la "prova dell'età" (ad esempio una banca, un operatore telefonico, un ente pubblico o un soggetto privato) che, ove non sia già destinatario di obblighi normativi di identificazione degli utenti, deve essere certificato per garantirne l'affidabilità, deve conoscere l'identità della persona ma non il sito on line al quale il minore ha intenzione di iscriversi, così come aspirano ad essere i sistemi "SPID dei minori" o l'*European Digital Identity Wallet*³⁹. Su richiesta il terzo deve fornire all'utente "la prova dell'età" con adeguata certificazione priva di alcun dato che consenta di identificarlo; l'utente deve inviare la "prova dell'età" al sito o alla piattaforma, chiamata invece a verificare l'autenticità della "prova dell'età" e i requisiti per consentire l'accesso ai propri contenuti o servizi.

Secondo AGCOM, tale modello può costituire il migliore bilanciamento tra gli interessi in gioco, tra cui il minor trattamento dei dati personali, garantendo l'efficacia del riconoscimento e la tutela dei minori.

In particolar modo, si evidenzia come AGCOM, pur adottando un approccio in parte differente rispetto al Garante privacy, abbia comunque inteso, almeno fino ad oggi, non indicare perentoriamente il tipo di tecnologia da impiegare, quanto invece delineare un insieme di principi, sicuramente più stringenti, attraverso la proposta di un modello di procedimento attuabile mediante strumenti e soggetti differenti.

Ciò è da considerare sicuramente con favore e per diverse ragioni: *in primis* perché, così come il Garante privacy, AGCOM non ha inteso optare per una specifica tecnologia, lasciando dunque i soggetti coinvolti, compresi gli sviluppatori delle

digitale) ed offline, sul consenso dei genitori, sull'attestazione demandata a terzi, sull'utilizzo di app specifiche, sull'impiego del numero di telefono e della email (e sui dati ivi registrati) e infine sull'utilizzo dei dati bancari qualora esistenti o comunque presenti in database certificati.

39. Approfondisce l'argomento MARTONI 2022.

tecnologie, liberi nell'*iter* decisionale, seppure sulla base di specifiche direttive; ciò sicuramente avvantaggia lo sviluppo delle tecnologie, consentendo allo stesso tempo il loro adeguamento rispetto al singolo contesto e all'evoluzione, sociale, economica, giuridica e tecnologica. Dall'altra parte, invece, ciò consente di adeguare gli strumenti ai soggetti utilizzatori, quindi i minori che, quali nativi digitali possono in alcuni casi essere in grado di eludere le tecnologie stesse e, addirittura, superarle.

3. Brevi osservazioni conclusive

L'uso di strumenti tecnologici al fine di verificare l'età dei minori che accedono online ed esprimono un proprio autonomo consenso può incontrare due ordini di problemi che è possibile ricondurre al più ampio concetto di "obsolescenza tecnologica": la tecnologia, in quanto tale, va infatti incontro al suo stesso superamento sia in ragione dello sviluppo di altre tecnologie, in grado di renderla obsoleta o eludibile, sia in ragione delle capacità della persona umana che, utilizzando le stesse tecnologie per più tempo, può divenire capace di aggirarla.

Per tali motivi, si rinnova la convinzione per cui, seppure l'uso delle tecnologie al fine della verifica dell'età sia sicuramente positivo, se non necessario, queste devono rappresentare allo stesso tempo un aiuto per le persone, in specie per i soggetti, quali i genitori o i tutori, chiamati ad operare un «corretto ruolo parentale, attento e consapevole. Un ruolo che si permea di doveri di protezione e di controllo»⁴⁰ relativamente all'accesso alle tecnologie digitali da parte dei minori. A tal fine, dunque, si ritiene che debba essere recuperato e anzi valorizzato il ruolo dei genitori, in generale dei soggetti

che affiancano i minori, sia quali controllori delle attività online dei minori, sia quali educatori dei minori stessi, chiamati dunque ad individuare ed indicare l'uso dei migliori servizi digitali per lo sviluppo e la crescita dei minori di età⁴¹. Ciò, però, incontra la necessità, dovuta all'abbandono del c.d. "modello paternalistico" della responsabilità genitoriale, «di riequilibrare il rapporto tra il minore ed il genitore nell'esercizio dei suoi doveri, in particolare» di individuare «il massimo limite entro cui può spingersi il controllo genitoriale, ancorato alla garanzia del *best interest* del minore in virtù della sua vulnerabilità rispetto agli sconfinati rischi che celano queste attività»⁴².

Infatti, solo attraverso la diffusione di una "cultura" delle tecnologie digitali e una «alfabetizzazione digitale e mediatica»⁴³, diretta sia ai minori che ai genitori, comprensiva dei rischi e dei vantaggi che ne derivano, anche attraverso un precipuo intervento delle istituzioni scolastiche⁴⁴, sarà effettivamente possibile fornire la necessaria educazione ed istruzione⁴⁵, tutelando i minori online e allo stesso tempo consentire un'esperienza d'uso positiva ed efficace e quanto più possibilmente aderente alle proprie capacità, aspettative e volontà, recuperando il ruolo che riveste, al contempo, l'eventuale dissenso espresso dal minore, anche quando non ne era legalmente capace, nonché l'eventuale revoca esercitata successivamente in costanza di capacità⁴⁶.

40. IRTI 2019, p. 633.

41. In tema, *ex multis* si rimanda a THIENE 2019, p. 37 ss.

42. STELLA 2022, p. 1435.

43. SCIA 2019, p. 38, secondo il quale sarebbe opportuna una «alleanza nel settore dell'istruzione fra famiglie, scuola, società civile e parti interessate, compresi i soggetti operanti nei media e nei servizi audiovisivi, per garantire una dinamica equilibrata e proattiva tra mondo digitale e minori».

44. Sottolinea tale importante ruolo THIENE 2017.

45. Riflette sulla differenziazione tra educazione ed istruzione, in specie rispetto alla materia del digitale, CAMPAGNOLI 2019.

46. Infatti, a riguardo le linee guida in tema di espressione del consenso, emanate dall'EDPB, hanno specificato come il consenso prestato dal genitore per autorizzare il trattamento dei dati personali del minore perda efficacia al momento del raggiungimento della cosiddetta età del consenso, momento in cui egli sarà quindi chiamato a rinnovarlo o, diversamente, a revocarlo.

Riferimenti bibliografici

- AGCOM (2018), *Libro Bianco Media e Minori 2.0*, 2018
- AGCOM (2014), *Libro Bianco Media e Minori*, 2014
- G. ALPA (2004), *I contratti del minore. Appunti di diritto comparato*, in “Contratti”, 2004, n. 5
- E. ANDREOLA (2019), *Minori e incapaci in Internet*, Edizioni Scientifiche Italiane, 2019
- E. BATTELLI (2022), *Privacy e minori: l'inadeguatezza del c.d. consenso digitale*, in M. D'Auria (a cura di), “I problemi dell'informazione nel diritto civile, oggi. Scritti in onore di Vincenzo Cuffaro”, Roma TrE-Press, 2022
- M. BIANCA (a cura di) (2021), *The best interest of the child*, Sapienza University Press, 2021
- F. BRAVO (2017), *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in G. Finocchiaro (diretto da), “Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali”, Zanichelli, 2017
- D. CACCIOPPO (2024), *Sharenting e tutela dei dati personali del minore: profili giuridici di un fenomeno interdisciplinare*, in “Rivista italiana di informatica e diritto”, 2024, n. 2
- I.A. CAGGIANO (2018), *Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione*, in “Familia”, 2018, n. 1
- M.N. CAMPAGNOLI (2019), *Diritto all'educazione e nuove tecnologie. Sulla necessità di un approccio consapevole*, in “dirittifondamentali.it”, 2019, n. 2
- G. CAPILLI (2024), *Minori in rete tra consenso e verifica dell'età. Analisi comparata e proposte di adeguamento al GDPR*, in “MediaLaws”, 2024, n. 1
- G. CAPILLI (2012), *La capacità negoziale dei minori. Analisi comparata e prospettive di riforma*, Giappichelli, 2012
- M. CINQUE (2007), *Il minore contraente. Contesti e limiti della capacità*, Cedam, 2007
- C. DI COSTANZO (2023), *La tutela costituzionale del minore: identità, salute e relazioni*, in P. Caretti, U. De Siervo, M.C. Grisolia (a cura di), “Osservatorio sulle fonti. Collana di studi”, Giappichelli, 2023
- EUROPEAN DATA PROTECTION BOARD (2020), *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, 4 maggio 2020
- R. GIARDA, J. LIOTTA, G. RINDI (2022), *Vita quotidiana del minore online. Tra esigenze di tutela e limiti tecnologici*, in “MediaLaws”, 2022, n. 1
- C. IRTI (2019), *Persona minore di età e libertà di autodeterminazione*, in “Giustizia civile”, 2019, n. 3
- E. LAMARQUE (2023), *Pesare le parole. Il principio del best interest of the child come principio del migliore interesse del minore*, in “Famiglia e Diritto”, 2023, n. 4
- E. LAMARQUE (2016), *Prima i bambini. Il principio del best interest of the child nella prospettiva costituzionale*, Franco Angeli, 2016
- D. MARCELLO (2022), *Il trattamento dei dati digitali del minore*, in “Actualidad Jurídica Iberoamericana”, 2022, n. 17 bis
- M. MARTONI (2022), *Il minore sulla soglia dell'onlife. Questioni di identificazione elettronica e di age verification: SpID per i minori e lo European Digital Identity Wallet*, in “federalismi.it”, 2022, n. 26
- M. MARTONI (2021), *I diritti dei minori e i rischi connessi all'esposizione a contenuti on-line pericolosi. Primi spunti per una riflessione etico-giuridica sulla protezione prioritaria del minore quale presupposto di una società moderna sostenibile*, in “Notizie di Politeia”, 2021, n. 144

- M. MARTONI (2020), *Datificazione dei nativi digitali e società della classificazione. Prime riflessioni sull'educazione alla cittadinanza digitale*, in "federalismi.it", 2020, n. 1
- F. NADDEO (2018), *Il consenso al trattamento dei dati personali del minore*, in "Il Diritto dell'informazione e dell'informatica", 2018, n. 1
- M. OROFINO (2018), *Minori e diritto alla protezione dei dati personali*, in M. Orofino, F. Pizzetti (a cura di), "Privacy, minori, cyberbullismo", Giappichelli, 2018
- M.L. PADELLETTI (2018), *Salvaguardia dei minori e best interests of the child secondo la Convenzione di New York sui diritti del fanciullo*, in "La comunità internazionale: rivista trimestrale della Società Italiana per l'Organizzazione Internazionale", 2018, n. 3
- F. PANUCCIO DATTOLO (2009), *Minori e internet*, Giappichelli, 2009
- S. RODOTÀ (1995), *Tecnologie e diritti*, il Mulino, 1995
- F. SCIA (2019), *Riservatezza e oblio. Diritti dei minori e servizi della società dell'informazione*, in "European Journal of Privacy Law & Technologies", 2019, n. 2
- F. SCIA (2018), *Riservatezza e oblio: i diritti dei minori nell'era di internet e dei social networks*, in "Innovazione e diritto", 2018, n. 4
- G. SCORZA (2023), *Appena nati e già online*, in "Specchio", 8 gennaio 2023, e sul sito dell'[Autorità garante per la protezione dei dati personali](#)
- R. SENIGAGLIA (2020), *Minore età e contratto. Contributo alla teoria della capacità*, Giappichelli, 2020
- G. SPOTO (2016), *Disciplina del consenso e tutela del minore*, in S. Sica, V. D'Antonio, G.M. Riccio (a cura di), "La nuova disciplina europea della privacy", Cedam, 2016
- P. STANZIONE, G. SCIANCALEPORE (2006), *Minori e diritti fondamentali*, Giuffrè, 2006
- E. STELLA (2022), *Il best interest del minore tra società dell'informazione e responsabilità genitoriale nella disciplina italiana. Interventi normativi e novità rimediali*, in "Actualidad Jurídica Iberoamericana", 2022, n. 17 bis
- A. THIENE (2019), *Gioventù bruciata on line: quale responsabilità per i genitori?*, in A. Annoni, A. Thiene (a cura di), "Minori e privacy. La tutela dei dati personali dei bambini e degli adolescenti alla luce del Regolamento (UE) 2016/679", Jovene, 2019
- A. THIENE (2017), *I diritti della personalità dei minori nello spazio virtuale*, in "Annali online della Didattica e della Formazione Docente", 2017, n. 13

Sezione monografica

Cittadini e pubbliche amministrazioni tra AI e diritto all'umano

a cura di
Enrico Carloni



ENRICO CARLONI

Dalla legalità algoritmica alla legalità (dell'amministrazione) artificiale. Premesse ad uno studio

L'avvento delle intelligenze artificiali, ora nella forma delle AI generative, come ChatGPT, pone problemi formidabili ed al tempo stesso offre straordinarie opportunità di miglioramento dell'azione pubblica. La questione, dal punto di vista del diritto amministrativo, è quella di comprendere il fenomeno e quindi riflettere su quali regole possano continuare a garantire l'individuo nel rapporto con il nuovo potere digitale. Dottrina, legislatore e, soprattutto, giurisprudenza, negli anni recenti hanno delineato i fondamenti di una nuova legalità algoritmica: il saggio riflette, in termini introduttivi, sulla "tenuta" di quei principi (di trasparenza, non esclusività, non discriminazione) e sulla loro effettiva "consistenza" a fronte delle nuove prospettive di "amministrazione artificiale" (intendendo con questo l'amministrazione che fa ricorso, per le sue decisioni, a soluzioni avanzate di intelligenza artificiale).

*Amministrazione digitale – Intelligenza artificiale – Decisione automatizzata – Legalità algoritmica
Amministrazione artificiale*

From algorithmic legality to artificial (administrative) legality. Preliminary reflections for a study

The advent of artificial intelligence, now in the form of generative AI, such as ChatGPT, poses formidable problems and at the same time offers extraordinary opportunities for improving public action. The question, from the point of view of administrative law, is to understand the phenomenon and therefore reflect on which rules can continue to guarantee the individual in the relationship with the new digital power. Doctrine, legislator and, above all, jurisprudence, in recent years have outlined the foundations of a new algorithmic legality: the essay reflects, in introductory terms, on the "hold" of those principles (of transparency, non-exclusivity, non-discrimination) and on their actual "consistency" in the face of the new prospects of "artificial administration" (meaning by this the administration that uses, for its decisions, advanced artificial intelligence solutions).

*Digital administration – Artificial intelligence – Automated decision-making – Algorithmic legality
Artificial administration*

L'Autore è professore ordinario di Diritto amministrativo presso il Dipartimento di Scienze politiche dell'Università di Perugia

Questo contributo fa parte della sezione monografica *Cittadini e pubbliche amministrazioni tra AI e diritto all'umano*, a cura di Enrico Carloni

SOMMARIO: 1. Premessa. – 2. Verso la piena digitalizzazione. – 3. Governare nella rapidità delle trasformazioni. – 4. Fenomeni e definizioni: l'amministrazione algoritmica e l'impatto delle AI. – 5. I limiti della legalità algoritmica di fronte alle AI. – 6. Considerazioni problematiche a partire dall'art. 30 del Codice dei contratti. – 7. Amministrazione artificiale e diritto dell'amministrazione artificiale. – 8. Spunti per proseguire.

1. Premessa

L'amministrazione digitale, promessa almeno da vent'anni, è stata a lungo un miraggio, e mentre si accelera per giungere alla sua realizzazione, l'avvento delle intelligenze artificiali ed il loro annunciato utilizzo in ambito pubblico ci consegnano uno scenario che può apparire a buona ragione futuristico. Una utopia, o una distopia a seconda di come ci si ponga di fronte a queste trasformazioni, più che una realtà. Non fosse che l'innovazione è ormai intorno a noi, è qualcosa che sempre più non solo avvertiamo ma pratichiamo, ed è per questo che sentiamo l'incedere di una trasformazione che non può certo arrestarsi di fronte alla lentezza, ed ai ritardi, delle dinamiche di innovazione applicate alle amministrazioni.

Ogni trasformazione pone delle sfide, ed in particolare il passaggio da un'amministrazione "analogica" ad un'amministrazione "automatizzata" presenta opportunità ma anche rischi, che sta al diritto regolare per continuare ad assicurare tutele a chi è coinvolto nel rapporto con il potere, non ultimo il nuovo potere computazionale pubblico¹.

Da qui l'esigenza, che attraversa questa sezione monografica della Rivista, di analizzare una serie di questioni aperte dalle trasformazioni in corso, prendendo sul serio l'evoluzione tecnologica come fattore di cambiamento del modo di essere

e di operare delle amministrazioni e delle istituzioni. Certo l'impatto del cambiamento tecnologico pone una serie formidabile di problemi di garanzia: nel processo e nel procedimento. Pone sfide all'individuo spesso solo astrattamente in grado di controllare macchine che assumono uno spazio decisionale che rischia di essere sostanzialmente ad esse pienamente rimesso: questo perché la supervisione umana rischia di tradursi in subalternità, perché le competenze a disposizione dei funzionari sono inadeguate, perché l'algoritmo e le AI sono definiti al di fuori del contesto pubblico che pure li utilizzerà nella sua azione. Se l'algoritmo è criterio del potere, come ci ricorda Crawford² (e come ben rimarca Ponti³), riflettere sulle condizioni del suo legittimo utilizzo nel sistema pubblico è decisivo ed in questa direzione vanno, per frammenti diversi rispetto ad un discorso di straordinaria complessità, i saggi raccolti in questa sezione. La questione centrale è cogliere le trasformazioni nella prospettiva dell'effettività dei diritti degli individui, posti di fronte alle nuove forme di potere che anche i soggetti pubblici iniziano ad utilizzare.

Il fiorire di scritti e iniziative su questi temi ci mostra che è il momento per riflettere criticamente su queste trasformazioni, e sul sistema pubblico che ne è attraversato ora passivamente ora come

1. Si v. diffusamente FALCONE 2023.

2. CRAWFORD 2021.

3. Sui problemi connessi, in particolare, alla tendenziale "estraneità" all'amministrazione del processo di produzione dell'algoritmo (e quindi ai suoi criteri di fondo), cfr., in questa sezione della Rivista, PONTI 2024.

protagonista⁴. La qual cosa può però apparire quasi paradossale se pensiamo alle difficoltà che ancora conosce il percorso della (piena) digitalizzazione pubblica.

Convivono certo, nel sistema amministrativo, e tanto più in quello italiano, fasi diverse: mentre la spinta alla digitalizzazione ancora trova formidabili resistenze, e quindi ancora tarda il pieno affermarsi dell'amministrazione digitale, osserviamo ambiti nei quali l'innovazione, nelle sue forme più *disruptive*, viene praticata attraverso il ricorso ad intelligenze artificiali. Come nella "Storia di due città", di Dickens, lo stesso tempo si presenta in forme profondamente diverse al mutare dei contesti, e mentre la transizione alla piena digitalizzazione si confronta con formidabili inadeguatezze del tessuto amministrativo, al contempo osserviamo l'utilizzo, spesso ancora sperimentale ma sempre meno episodico, di intelligenze artificiali anche da parte delle pubbliche amministrazioni.

Certo il ritardo, il *divario*⁵ tra la digitalizzazione *media* attesa e quella praticata, costituisce un dato problematico che accompagna inevitabilmente il discorso sull'evoluzione tecnologica applicata al sistema pubblico, ed è qualcosa con cui dobbiamo fare i conti nel mentre ci confrontiamo con le sfide della nuova amministrazione artificiale. L'amministrazione sarà, per un tempo forse lungo, al tempo stesso in affanno sul fronte della piena digitalizzazione (e, quindi, ancora non sarà un'amministrazione digitale), ma al contempo già inizierà ad essere, e dovrà essere per rispondere al suo ruolo, un'amministrazione ad un più avanzato stato di maturazione, in grado di utilizzare le intelligenze artificiali per l'esercizio delle proprie funzioni⁶. Un'amministrazione artificiale, appunto.

I due processi sono dunque naturalmente, ma non necessariamente, consequenziali ed il sistema procede a macchie di leopardo, come spesso accade al sistema amministrativo italiano. Da qui l'esigenza di confrontarci, e riflettere, sulle condizioni di sostenibilità (giuridiche, organizzative, di capacità) che permettono di affrontare queste trasformazioni.

2. Verso la piena digitalizzazione

Pur tra ritardi, che segnalano la persistente difficoltà del sistema italiano, l'ordinamento però evolve e le riforme si susseguono⁷: il PNRR pone al centro delle strategie di intervento proprio i processi di piena transizione digitale⁸, finanziando in modo consistente interventi e sostenendo ulteriori politiche di riforma. La piena digitalizzazione diviene possibile, e a volte praticata, presentando però non solo vantaggi ma nuovi divari. Nuove rigidità che sostituiscono le vecchie. Nuove forme di disumanizzazione e perdita di empatia finché le macchine operano secondo schemi rigidamente pre-imposti e standardizzanti. Il tutto nell'incapacità del pubblico di proporre insieme, al di là della retorica riformistica che le accomuna, semplicità di uso e digitalizzazione (sul versante dei servizi, ma non solo). Quasi a consegnarci uno scenario nel quale, persa l'elasticità pragmatica che ancora lo scenario analogico consentiva, un sistema troppo complesso anzitutto in termini normativi rischia di scariarsi senza mediatori in *form* digitali, perdendo quel "temperamento" che passava per l'azione e la comprensione del funzionario.

L'affermazione sempre più piena dei principi di *digital by default*, costruzione dei servizi intorno all'utente, "*once only*"; la rottura progressiva dei silos che contrassegnavano la ancora recente

4. L'ampiezza di scritti sul tema impedisce in effetti di fornire riferimenti bibliografici esaustivi. Si rimanda per questo anzitutto ai saggi contenuti in questa sezione monografica della Rivista, ed ai relativi approfondimenti. In termini generali, si può partire ai nostri fini da: CERRILLO MARTINEZ-PONCE SOLE 2024; LALLI 2024; BELISARIO-CASSANO 2023; TORCHIA 2023; MARCHETTI 2022, p. 323 ss.; CAVALLO PERIN-GALETTA 2020. Sulla legalità algoritmica, ci sia consentito rinviare tra gli altri, per un inquadramento del tema nelle sue coordinate oramai "tradizionali" a CARLONI 2020.

5. Cfr., per es., SGUEO 2022; CARLONI 2019.

6. Per questa nozione cfr. CARLONI 2024-A.

7. Tra gli altri cfr. MARCHETTI 2022; PIRAS 2020.

8. Sulla strategia di digitalizzazione del Piano, e la connessa "accelerazione", cfr., per es., SANTACROCE 2023; SAPORITO 2023; GALETTA 2022; PONTI 2022, p. 401 ss.

stagione delle "città-Stato digitali"; l'ingresso di piattaforme comuni e di basi di dati condivise, l'interoperabilità come criterio portante; il ricorso (non privo di problematicità) a soluzioni "*cloud by default*". Tutte queste trasformazioni che interessano la maturità dell'amministrazione digitale pongono le premesse per un'amministrazione artificiale in grado di disporre davvero di un potere digitale che attende di essere valorizzato con il ricorso a soluzioni di automatizzazione evoluta.

Nel campo, settoriale ma trasversale e dalle implicazioni sistemiche, dei contratti pubblici⁹, la digitalizzazione del ciclo di vita dei contratti è oramai pienamente affermata (nella sua forma, radicale, del *digital only*) e porta con sé la piena transizione ad una esclusività digitale che resta ancora difficile da perseguire in altri campi, ed anche qui invero problematica. D'altra parte, proprio in questo campo, le difficoltà incontrate dalle amministrazioni nella transizione alla piena digitalizzazione sono a confermare resistenze e ritardi, che rendono il percorso seppure in evidente evoluzione al tempo stesso sofferto.

L'eterno ritardo dell'amministrazione è forse in via di superamento, ma restano incertezze, situazioni differenziate, diversi livelli di capacità nel proporsi nel nuovo scenario: l'inevitabile scetticismo con il quale ci poniamo di fronte alle trasformazioni porta però con sé il rischio di sottovalutare i rischi connessi alla transizione.

D'altra parte, proprio il ritardo (il decennio di ritardo che l'Italia presenta costantemente, che già Giannini riscontrava sul finire degli anni Settanta del secolo scorso¹⁰) può ingenerare l'idea, fallace, di trasformazioni che sono ancora lontane dal concretizzarsi, rispetto alle quali deve dunque prevalere la spinta verso il completamento rispetto ad un approccio precauzionale o attento ai rischi connessi alle dinamiche di modernizzazione.

Confermando l'assunto di Giannini che voleva legate in modo indissolubile innovazione amministrativa ed innovazione tecnologica¹¹, il nuovo

scenario non pare destinato a passare sull'amministrazione senza toccarla e a ben vedere già si possono cogliere segnali di queste trasformazioni. Nel mentre ancora tarda il pieno passaggio del sistema amministrativo nel suo complesso alla piena digitalizzazione, alla piena realizzazione del modello di "amministrazione digitale" promesso da riforme di quasi vent'anni addietro, ecco dunque farsi largo un nuovo modello, quello di un'amministrazione non solo compiutamente digitale, ma aperta all'utilizzo di AI per l'esercizio delle sue funzioni: una "amministrazione artificiale"¹². Si può calare in questo campo l'osservazione di Rodotà relativa al cambiamento indotto dall'innovazione tecnologica in grado di incidere "profondamente" sul modo in cui (la sfera politica, per Rodotà, la "sfera amministrativa" per noi) «non solo si presenta, ma si struttura»¹³.

3. Governare nella rapidità delle trasformazioni

Le sollecitazioni sono in ogni caso ormai troppe, e l'incedere dei fenomeni al contempo troppo rapido e troppo pressante perché il sistema pubblico, pur con le sue inefficienze, non sia portato a confrontarsi: questo, certo, con un andamento che non riesce ad essere omogeneo, comune alle amministrazioni nel loro insieme. Interessa il centro prima della periferia, alcuni settori prima di altri, si sviluppa con soluzioni straordinariamente innovative che convivono con sacche di ritardo anche nell'introduzione di soluzioni banali di *e-governement*. Siamo in una età di passaggio, che va presidiata perché in questo campo, come vedremo, più che altrove vale l'ammonimento di Gramsci: «il vecchio mondo sta morendo. Quello nuovo tarda a comparire. E in questo chiaroscuro nascono i mostri».

«Nei prossimi dieci, forse nei prossimi cinque anni, vedremo più cambiamenti tecnologici di quanti ne abbiamo visti negli ultimi cinquanta

9. V., per es., CAVALLO PERIN-LIPARI-RACCA 2024; MATTARELLA-MARCHETTI 2024; CARULLO 2023; RACCA 2023; cfr. PONTI 2023.

10. Sulla "ricorrenza" di questo ritardo v., per es., CARLONI 2019.

11. Cfr. in questo senso NATALINI 2006.

12. CARLONI 2024-A.

13. RODOTÀ 2009.

anni»¹⁴: mentre le AI già irrompono nella vita di ciascuno attraverso le forme delle intelligenze di base e generative (GAI¹⁵), come ChatGTP, lo *sce-nario* che prefigura il Presidente Joseph R. Biden nel definire la strategia dell'Amministrazione statunitense ci consegna l'immagine di un'evoluzione che è ben lungi dall'essere arrivata alla sua maturità e ancora lontana dal dare segni di rallentamento.

Non è un caso se, anche dal punto di vista *perife-rico* dell'Italia, giudice, legislatore, dottrina, si confrontano in modo sempre più approfondito con le trasformazioni indotte dall'evoluzione tecnologica, seguendo un percorso che negli anni più recenti si è incentrato in particolare sulla sfida posta dalle decisioni amministrative automatizzate¹⁶. Decisioni frutto dell'utilizzo di algoritmi variamente complessi, rispetto alle quali è necessario ripensare meccanismi e regole di tutela.

Il punto è che quegli approdi, che sono ora codificati anche nelle nuove regole dei contratti pubblici, con i quali faremo i conti, rischiano di essere, seppure straordinariamente recenti nelle ultime affermazioni, già spiazzati da una innovazione che procede *troppo* rapidamente.

In un percorso che presenta dunque costantemente nuove sfide, l'avvento di modelli di base di intelligenza artificiale ("*AI foundation models*"), che vengono generalmente addestrati su vaste quantità di dati utilizzando l'apprendimento non supervisionato su larga scala, in grado di supportare attività a valle di ampia portata, molte delle quali potrebbero non essere state previste dagli sviluppatori, pone al diritto e alle stesse amministrazioni pubbliche questioni nuove, e interroga dunque in termini che richiedono di essere costantemente sottoposti a *critica* la nuova *amministrazione artificiale* che abbiamo di fronte (ora esattamente

innanzi a noi, ma che più spesso vediamo ancora in lontananza anche se in rapido avvicinamento).

Gli sviluppi, riprendendo il sottotitolo del libro di Luciano Floridi¹⁷, vanno di pari passo con le opportunità ed i rischi. Il primo rischio è quello di non riuscire correttamente a interpretare queste trasformazioni, proprio a causa della loro rapidità. Il secondo, quello di sottovalutare la dimensione umana e politica di trasformazioni che sono solo in parte artificiali, tanto che si discute del carattere davvero artificiale delle stesse AI e si avverte sull'esigenza (e la possibilità) di una prospettiva ancora umana prima che tecnologica che ne orienti l'avvento.

Il tutto, nella consapevolezza che ciò che abbiamo di fronte è molto più sfidante di ciò che abbiamo alle spalle: siamo, come avverte tra gli altri Li Fei-Fei¹⁸ sull'orlo di una rivoluzione tecnologica che ha il potere di rimodellare la vita come la conosciamo, che va compresa, interpretata, guidata perché sia incentrata sugli esseri umani. Questo, tanto più nella prospettiva dell'amministrazione, e quindi del cittadino al centro del nuovo paradigma dell'amministrazione artificiale.

4. Fenomeni e definizioni: l'amministrazione algoritmica e l'impatto delle AI

La questione, anche da una prospettiva giuridica, è legata anzitutto alla natura del fenomeno: nell'approccio delle AI si assiste infatti al passaggio da logiche di tipo deduttivo a logiche di tipo statistico-probabilistico: il sistema artificiale apprende, a partire dai dati, e così facendo migliora la propria capacità predittiva, secondo dinamiche nelle quali la "ricetta" (l'algoritmo) non opera in modo prevedibile e deterministico, ma evolve le sue strategie decisionali con l'esperienza.

14. THE WHITE HOUSE, *Remarks by President Biden and Vice President Harris on the Administration's Commitment to Advancing the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, October 30, 2023.

15. Si tratta di uno sviluppo potente e innovativo nel campo dell'intelligenza artificiale: esempi sono BERT (Google), GPT-4 (OpenAI), Llama2 (MetaAI). Questi modelli sono resi accessibili tramite strumenti come ChatGPT, Google Gemini e Microsoft Copilot. Alcuni modelli di basi di intelligenza artificiale hanno persino capacità robotiche come RoboCat di DeepMind (BOUSMALIS –VEZZANI–RAO et al. 2023).

16. La dottrina sul punto è molto ampia, si v. per tutti PREVITI 2022; CARLONI 2020; NAPOLI 2020; AVANZINI 2019; BRIGANTE 2019. Cfr. più diffusamente, in questa sezione della Rivista, spec. FORGIONE 2024; NAPOLI 2024.

17. FLORIDI 2022.

18. FEI FEI 2024.

Il problema è che la “cassetta degli attrezzi” che l'ordinamento ha approntato (o iniziato ad approntare), ammettendo l'ingresso nella decisione amministrativa di percorsi di decisione “automatizzata” viene costruita intorno all'idea di decisione algoritmica-deterministica (ancorché complessa). Vale la pena qui ripercorrere gli snodi centrali del ragionamento del giudice amministrativo che con le sentenze di pochi anni addietro ha aperto la strada (seguendo in questo, va detto, i traccianti già prefigurati dalla dottrina giuspubblicistica¹⁹) ed ammesso che le potenzialità offerte dalla automatizzazione dovessero trovare spazio nell'azione delle amministrazioni anche laddove il loro ingresso fosse risultato non pienamente coerente con tutte le specifiche disposizioni e garanzie definite per la amministrazione “analogica” e contenute in particolare nella legge sul procedimento amministrativo²⁰.

Ecco allora prefigurarsi i principi della nuova legalità algoritmica (attinenti alla imputabilità all'amministrazione, alla trasparenza come conoscibilità del carattere automatizzato della decisione e come comprensibilità della logica utilizzata, della non discriminazione, della non esclusività²¹).

Il cuore di questa nuova legalità si rinviene, come è noto (ma non sempre chiaro), in sentenze maturate intorno all'utilizzo di soluzioni di automatizzazione del tipo meno complesso: algoritmi di tipo deterministico che, seppure non rispondenti alle più tradizionali soluzioni di mera meccanizzazione di operazioni semplici e ripetitive, consentivano una chiara imputabilità delle scelte all'amministrazione (ed ai responsabili delle istruzioni algoritmiche) ed ancora una trasparenza dei criteri, delle indicazioni che guidano le scelte (*if... then...*) della “ricetta” algoritmica. Pur nella complessità data dalla quantità di dati processati e di variabili prese in considerazione, l'algoritmo produce un risultato che è verificabile, ripetibile, riconducibile ai criteri predeterminati che ne guidano il funzionamento: è allora ben possibile, per

un utente esperto, comprenderne la logica di funzionamento, verificarne il funzionamento (“accedendo” all'algoritmo) e quindi gli eventuali errori, provare a sindacarne i *bias* e operare su questo una supervisione umana.

La definizione ed il perfezionamento di questi principi, cumulandosi alla strategia europea di tipo precauzionale e orientata al rischio ma centrata sul “prodotto” AI (e non sul suo utilizzo in decisioni pubbliche)²², si presume consenta di immaginare un percorso di costruzione di tutele “adeguato” ancorché non pienamente conforme ai parametri legali tradizionali ancora iscritti nelle leggi sul procedimento (ed in particolare, per quello che qui interessa, nella legge n. 241 del 1990).

L'idea, che accompagna la giurisprudenza amministrativa su questi temi e sembra orientare ancora la costruzione della legalità connessa all'uso di AI, cui cominciamo a trovarci di fronte, in continuità con la legalità dell'amministrazione algoritmica, è che questo passaggio non sia decisivo nel segnare una crisi dei nuovi principi: la trasparenza sarà certo sempre più relativa alla “logica” algoritmica, ma potrà ancora fornire coordinate di tutela perché relativa ai dati utilizzati, all'addestramento della macchina, ai criteri che ne guidano le costruzioni inferenziali. E da qui sarà ancora possibile assicurare, o almeno provare a verificare, il carattere non discriminatorio delle scelte, e questo in particolare grazie a una supervisione umana in grado ancora di osservare il funzionamento dei sistemi e nel caso smentirne gli esiti.

5. I limiti della legalità algoritmica di fronte alle AI

La questione è essenzialmente questa: una simile legalità algoritmica, suscettibile di essere valutata come adeguata rispetto a decisioni algoritmiche complesse ma comunque sulla scorta di una predeterminazione “umana” dei parametri rilevanti e quindi secondo logiche essenzialmente (se non

19. V. per tutti CIVITARESE MATTEUCCI 2019; SIMONCINI 2019.

20. Specificamente sulla trasparenza amministrativa algoritmica e le sue plurali declinazioni, CARLONI 2023. Specificamente sul problema della *explainability* cfr., per es., LONGO 2022.

21. Sulla questione della “riserva di umanità” e dello “human in the loop”, cfr., per es., MARCHETTI 2021, e più recentemente MARTIRE 2024, GALETTA 2023, GALLONE 2023.

22. Diffusamente su questi temi, in questa sezione della Rivista, NAPOLI 2024, e FORGIONE 2024 (cui si rinvia anche per i puntuali riferimenti giurisprudenziali e dottrinali).

esclusivamente) deterministiche, resta adeguata anche a fronte di decisioni rimesse in modo sempre più autonomo ad agenti virtuali che operano secondo schemi non deterministici ma statistico-probabilistico e predittivo?

L'ambizione della giurisprudenza, colta però qui attraverso *obiter dictum* più che decisioni e soprattutto interpretata alla luce di un'evoluzione normativa guidata dalla stessa matrice giurisprudenziale (il Codice dei contratti, che all'art. 30 parla ora per la prima volta di intelligenze artificiali e del loro utilizzo nell'ambito della decisione pubblica), pare essere quella di poter proiettare i principi della legalità algoritmica sulla decisione frutto di intelligenze artificiali. Con questa ambizione, o illusione, dobbiamo confrontarci criticamente.

Il fatto è che le AI si emancipano progressivamente dalla stessa idea di algoritmo (che il recente disegno di legge del Governo definisce come una «sequenza finita ed ordinata di operazioni, o istruzioni, progettate per raggiungere un obiettivo specifico») ed acquisiscono una autonomia che è crescente, e formidabile nel caso delle AI di tipo generale e generativo. L'incalzare dell'evoluzione tecnologica, frutto questa sì di scelte profondamente umane a partire dalla progressiva perdita di prudenza e cautela nell'inseguire uno sviluppo vorticoso accompagnandolo con investimenti relevantissimi (specie privati), ci consegna quotidianamente fenomeni di complessità crescente. Si può sintetizzare il discorso intorno all'avvento di ChatGPT, già in seconda fila rispetto a sistemi più avanzati che lo stanno soppiantando ma punto di svolta nell'affermazione dell'AI generativa e del suo utilizzo come fenomeno di massa. Nel disegno di legge governativa per AI si intende «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali»: si capisce bene che la nozione di AI raccoglie fenomeni diversi che non

è già difficile comprendere, inquadrare²³ ed ancor più complesso governare. La questione da tenere sempre presente è, in questo scenario, non solo la complessità crescente e l'evoluzione per stadi che spesso creano delle discontinuità (come inadeguatezza dei precedenti paradigmi nel definire e regolare i fenomeni), ma la rapidità delle trasformazioni in atto.

Si può comunque ripartire dalla decisione del Consiglio di Stato che propone di distinguere tra algoritmi «semplici» («una sequenza finita di istruzioni, ben definite e non ambigue, così da poter essere eseguite meccanicamente e tali da produrre un determinato risultato»), ed intelligenza artificiale. Nel caso delle AI, «l'algoritmo contempla meccanismi di *machine learning* e crea un sistema che non si limita solo ad applicare le regole software e i parametri preimpostati (come fa invece l'algoritmo «tradizionale») ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico»²⁴.

Si coglie, nella giurisprudenza e nella stessa legislazione, l'idea che le regole di legalità algoritmiche possano proiettarsi dalla decisione «algoritmica» alla decisione «artificiale»: questo perché le macchine operano nel secondo caso con margini di autonomia («non si limita solo ad applicare regole preimpostate») ma restano comunque guidate da criteri di fondo definiti dall'uomo, attraverso la fissazione dei parametri decisionali, la selezione delle basi di dati rilevanti, l'addestramento delle AI. ChatGPT ci pone di fronte allora ad un problema diverso, ad un «terzo tipo» di automatizzazione, e la questione è appunto se le regole pensate per il «primo tipo» (decisione algoritmica), progettate con fiducia su decisioni prese attraverso soluzioni del «secondo tipo» (AI «specializzate», operanti con margini di autonomia e autoapprendimento ma entro criteri fondamentali noti e predefiniti, ad addestramento supervisionato dall'uomo), possano ancora reputarsi consistenti a fronte di intelligenze artificiali del «terzo tipo».

23. Cfr. sul punto, per es., CAVALLO PERIN-ALBERTI 2020. Sull'esigenza di dialogo tra tecnologia e diritto, ed in particolare su quella di una lettura «tecnologicamente orientata» del diritto, cfr. CAVALLO PERIN 2020.

24. In questo senso si v. Cons. Stato, sez. III, 25 novembre 2021, n. 7891; si v. già (specie per la nozione di algoritmo «semplice» poi ripresa dal giudice di secondo grado) in prima cura Tar Lombardia, Milano, sez. II, 31 marzo 2021, n. 843.

6. Considerazioni problematiche a partire dall'art. 30 del Codice dei contratti

Queste riflessioni possono essere calate su una specifica previsione normativa, che si pone nel momento attuale come "sonda" di un approccio aperto all'ingresso delle AI nel cuore della decisione amministrativa. Il riferimento è all'art. 30 del Codice dei contratti²⁵, d.lgs. n. 36 del 2023, che testualmente recita (nel regolare il ricorso a "procedure automatizzate nel ciclo di vita dei contratti pubblici"): «1. Per migliorare l'efficienza le stazioni appaltanti e gli enti concedenti provvedono, ove possibile, ad automatizzare le proprie attività ricorrendo a soluzioni tecnologiche, ivi incluse l'intelligenza artificiale e le tecnologie di registri distribuiti, nel rispetto delle specifiche disposizioni in materia».

Tacendo delle altre previsioni, non certo per questo irrilevanti, dell'articolo e della complessiva Parte II del Libro I (parte relativa alla piena digitalizzazione del ciclo di vita dei contratti), merita attenzione il successivo comma 3: «le decisioni assunte mediante automazione rispettano i principi di: a) conoscibilità e comprensibilità, per cui ogni operatore economico ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino e, in tal caso, a ricevere informazioni significative sulla logica utilizzata; b) non esclusività della decisione algoritmica, per cui comunque esiste nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatizzata; c) non discriminazione algoritmica, per cui il titolare mette in atto misure tecniche e organizzative adeguate al fine di impedire effetti discriminatori nei confronti degli operatori economici».

In sostanza, l'art. 30 ci presenta un *condensato* dei principi cardine dalla nuova legalità algoritmica, dando veste legislativa non solo ai tre principi già richiamati ("trasparenza", "non esclusività", "non discriminazione"), ma anche dando esplicita copertura legislativa²⁶ all'uso di forme di potere automatizzato come modo di essere non solo "ordinario" dell'amministrazione, ma persino

"preferenziale" sia pure ad alcune condizioni. Preferenziale perché visto come in grado di assicurare un miglioramento dell'azione pubblica, condizionato perché comunque sottoposto al limite della necessaria garanzia dei principi: si può dire che se la decisione automatizzata, anche nella forma di decisione tramite AI, è in grado di rispondere ai tre principi di legalità algoritmica, allora la scelta della automatizzazione è non solo legittima ma preferibile in quanto meglio in grado di assicurare l'efficienza dell'azione pubblica e il raggiungimento del risultato.

Ci si può chiedere in via preliminare se questa formulazione (l'art. 30) parli solo all'amministrazione per contratti o si riferisca più complessivamente a regolare l'azione della "nuova amministrazione": ad avviso di chi scrive la risposta va nel senso di riconoscere all'art. 30 una portata non strettamente settoriale. Si tratta, come detto, d'altra parte della ri-formulazione di principi generali dell'ordinamento (come tali inquadrati dalla dottrina e desumibili/desunti dal GDPR) e di dare veste legale a principi giurisprudenziali sempre più consolidati (nella giurisprudenza ormai sul punto solida del giudice amministrativo).

La questione su cui soffermarsi è però specifica: nel trattare di "automatizzazione", il legislatore estende in modo forse troppo semplicistico il ragionamento alle AI quali soluzione di automazione («soluzioni tecnologiche [...] ivi inclusa l'intelligenza artificiale»), sottovalutando lo strappo, il salto di livello, che comportano alcune soluzioni di AI.

Il cambiamento tecnologico procede più rapidamente della capacità del diritto di irregimentarlo, intercettarlo e guidarlo: ci troviamo ora di fronte a soluzioni di AI che operano attraverso una rete neurale di parametri in grado di generare contenuti in modo largamente autonomo, in risposta agli input o ai *prompt*. Questi parametri si definiscono e perfezionano secondo percorsi di auto-addestramento e auto-apprendimento e sono numerosissimi (erano 117 milioni per ChatGPT, sono 175 miliardi in ChatGPT 3, che è poi quello

25. Su questa previsione, cfr., in questa sezione della Rivista, FORGIONE 2024. In termini generali, per cogliere la formulazione nel contesto che l'ha prodotta, si v. la *Relazione di accompagnamento al Codice dei contratti*, prodotta dalla speciale Commissione in seno al Consiglio di Stato (in Giustizia-amministrativa.it).

26. Sull'approccio giurisprudenziale già orientato a non ritenerla necessaria, v., per es., TORCHIA 2023.

comunemente utilizzato, sono circa 100 trilioni quelli di ChatGPT 4).

Ad un livello ancora solo introduttivo, la questione è questa: come possiamo assicurare che i principi di legalità algoritmica, sorti a partire da casi di automatizzazione retti da criteri deterministici (come nel caso delle assegnazioni di cattedre della “buona scuola”), possano continuare ad offrire una adeguata tutela all’individuo ed al tempo stesso restare “consistenti” rispetto ai nuovi fenomeni? Se è vera la prospettiva di Floridi, che presenta l’AI come un “divorzio” (tra la capacità di produrre un risultato efficiente e l’intelligenza necessaria per farlo), l’AI quanto più opera in autonomia, per inferenze, sulla base di parametri che costruisce ed applica, tanto più non può essere spiegata secondo una “logica” di ragionamento umano. Il dilemma della *AI explainability*²⁷ attiene a questo, ed alla difficoltà/impossibilità di descrivere ciò che avviene nella *black box* della AI in termini comprensibili per l’individuo²⁸.

Se questo è vero, ne derivano problemi formidabili per la tenuta dei principi di legalità algoritmica, che rischiano di essere dei vuoti proclami (da un lato) o delle condizioni impossibili da realizzare (dall’altro).

Pensiamo alla trasparenza: certo può ben essere assicurata la “conoscibilità” (come esplicitazione del ricorso ad un potere automatizzato), ma possiamo ancora immaginare che si possa assicurare “comprensibilità” sia pure nei termini non rigorosi della piena *explainability* ma in quelli più laschi (ma assunti come comunque adeguati) del diritto a ricevere “informazioni significative sulla logica utilizzata”? Pensiamo alla “non discriminazione”: se la macchina opera in campi diversi da quelli per i quali è stata addestrata, come riuscire a comprendere la presenza di *bias* algoritmici che evidentemente non derivano dai criteri e parametri che sono stati definiti per il suo funzionamento? Pensiamo alla supervisione umana: ferma l’esigenza di formidabili investimenti sulle competenze dei funzionari, e di rafforzamento della capacità di rapportarsi con questi strumenti degli

stessi cittadini, come ed in che termini possiamo davvero assicurare un “contributo umano capace di validare o smentire” la decisione automatizzata quando questa costituisce il risultato del tentativo di rispondere a domande complesse, utilizzando masse di dati che escono di norma dalla capacità di gestione umana “a vista”²⁹, applicando reti neurali che utilizzano una numero enorme di parametri?

7. Amministrazione artificiale e diritto dell’amministrazione artificiale

Posta in questi termini, la questione rischia di apparire irrisolvibile, ed i problemi disarmanti: non è questa la prospettiva da cui cogliere la sfida.

Va anzitutto preso atto, in modo consapevole, del fatto che le nuove tecnologie pongono problemi nuovi, ed il fatto che si sia iniziato a trovare soluzione a problemi simili (ma diversi) non deve portarci a pensare che le stesse soluzioni possano semplicemente essere meglio perfezionate per applicarsi a fenomeni che si pongono tra loro in continuità.

Ben venga, in sostanza, l’azione amministrativa automatizzata, frutto di algoritmi complessi difficili da conoscere e decifrare per il destinatario dell’azione pubblica ma non radicalmente inconoscibili. Ben venga, qui, la costruzione di una legalità algoritmica che, finché la natura delle soluzioni utilizzate lo consente, può proiettarsi sull’utilizzo di soluzioni di crescente complessità che possono essere anche ricomprese in una nozione “larga” di AI, ma continuano ad essere caratterizzate da una prevalenza del controllo umano. Ma nel mentre perfezioniamo questa cassetta degli attrezzi, della quale abbiamo sempre più bisogno perché sempre più spesso (per ragioni di efficienza, di ripetitività, di imparzialità, di costi pubblici nella gestione di procedure massive, ecc.) la decisione pubblica è in tutto o in parte “algoritmica”, dobbiamo cominciare a pensare a qualcosa di ancora diverso, che può forse partire dalla legalità algoritmica ma non arrestarsi certo ad essa.

Nella consapevolezza che da un lato si tratta di un problema che non si esaurisce nel perimetro

27. Tema al centro della riflessione delle diverse scienze interessate alla AI, non ultimo quelle giuridiche: cfr., per es., ARDUINI 2021; FALLETTI 2020; GIANNOTTI–PEDRESCHI 2019.

28. Sui problemi che ne derivano, anzitutto per il regolatore, cfr., per es., già EBERS 2020; BATHAEE 2018, p. 901 ss.

29. Su come questo problema di “complessità” sfidi il diritto, cfr., per es., BARBATI 2021; diffusamente DE DONNO–DI LASCIO 2022.

delle pubbliche amministrazioni, e che dall'altro si tratta di un'opportunità straordinaria per il miglioramento della capacità di risposta alle sfide contemporanee.

Ci troviamo di fronte a trasformazioni che richiedono adeguamenti normativi, sollecitano misure di regolazione, mettono in discussione le consuete coordinate di governo dei fenomeni, come ci mostrano i problemi emersi ad esempio nel campo della protezione della riservatezza, in quello del mercato del lavoro, in quello della proprietà intellettuale, in quello dei mercati finanziari. Basta guardarci intorno per cogliere l'impatto delle AI, che non a caso è al centro della riflessione delle diverse scienze (e non ultimo di quelle umane e sociali), e questo impatto trasformativo appare, per gli interpreti più attenti di queste dinamiche, solo l'embrione del cambiamento che ci attende nell'arco di pochi anni.

La pubblica amministrazione, persino quella italiana che pure appare a volte ancora lontanissima da questa prospettiva, a volte refrattaria ai processi di trasformazione indotti dalla tecnologia e in questo quasi pre-moderna, non sfugge dunque a queste trasformazioni. L'utilizzo di AI nel cuore della decisione amministrativa, sia essa pienamente sostitutiva del ruolo umano o anche co-pilota che definisce però in termini sostanziali il contenuto delle scelte, propone una diversa nozione, di *amministrazione artificiale*, che attende ancora una cornice di legalità che sia effettiva senza precluderne lo sviluppo.

L'amministrazione artificiale è d'altra parte non una chimera, ma una *pratica*: una mappatura condotta a livello di amministrazioni federali non militari statunitensi, ha rilevato oltre duemila esperienze concrete di utilizzo di AI nell'ambito della loro azione, e il dato è in costante e rapido incremento³⁰. Meno sistematica la mappatura delle, certo meno numerose, esperienze italiane, eppure anche qui il fenomeno è in costante evoluzione e

l'applicazione concreta di soluzioni di AI si accresce giorno per giorno.

L'intelligenza artificiale si riflette dunque in una nuova, e diversa, amministrazione, che ci appare al contempo ancora di là da venire eppure a ben vedere già presente.

Ed il diritto (anche il diritto amministrativo), a sua volta, non può ignorare la sfida di governare, o almeno tentare di farlo, questi processi, salvo porsi il problema, come ci avverte da ultimo Giusella Finocchiaro³¹, di capire "quali regole" siano adatte al fine. Si tratta infatti di un fenomeno troppo importante, «for both promise and peril»: in grado di produrre un impatto rilevante, sia che si colga dal lato della questione delle potenzialità sia che lo si faccia dal lato dei rischi³². Il che vale in via generale per il discorso sulla regolazione delle AI, ma vale in modo specifico per la regolazione delle AI in ambito pubblico, ed in particolare, nell'ambito dell'esercizio delle funzioni amministrative.

Quale il senso, la direzione, i rischi, di questa trasformazione colti dallo specifico punto di osservazione dell'attività delle pubbliche amministrazioni: si tratta evidentemente, in primo luogo, di una straordinaria opportunità, che va accolta senza chiusure, evitando irrigidimenti, ma procedendo ad occhi aperti nella consapevolezza dei rischi e della necessità di trovare anche *nel percorso* le soluzioni che ora non abbiamo. Si può discutere certo della percorribilità di questa trasformazione, ma ancor più del *come*: dei limiti rispetto a questa scelta (in quali ambiti, ad esempio, escludere la possibilità di ricorso ad AI), delle forme ammissibili (fino a che punto si può tollerare un ruolo dominante o esclusivo delle AI), dei pesi e contrappesi, delle forme di garanzia. Ed in questo senso vanno molti dei contributi in questa sezione della Rivista.

E occorre discutere, soprattutto, in questo quadro, di una problematica che è specifica ma centrale per il diritto amministrativo ed il diritto pubblico, quella dei diritti e delle tutele dell'individuo di fronte a queste forme nuove, o rinnovate,

30. Una mappatura è presentata come "*The Government is Using AI to Better Serve the Public*", dove è raccolto (ed è possibile scaricare) un inventario che consta di 2390 esperienze al 1° settembre 2023.

31. FINOCCHIARO 2024.

32. Dal che consegue, in particolare, che il fenomeno non può essere rimesso all'evoluzione del mercato e della tecnologia, entrambe nelle mani dei grandi player globali, gli "OTT" (*over the top*) dello scenario tecnologico: «Artificial intelligence is too important to be left entirely in the hands of the big tech companies»: FEI FEI-ETCHEMENDY 2023.

di esercizio del potere. L'amministrazione artificiale va dunque colta in termini non di rifiuto, ma comunque di critica consapevole: consci che questo stadio evolutivo della tecnica, nel quale la dimensione simbolica della idea di "intelligenza" rischia di portare con sé all'opposto un'accezione fideistica nel portato di miglioramento connesso alla introduzione delle nuove soluzioni.

8. Spunti per proseguire

Pur cogliendo la prospettiva dell'amministrazione digitale anche dal lato delle potenzialità, in sostanza, contraddicendo l'auspicio di Lee e Qiufan, non possiamo "non continuare a preoccuparci"³³: il che comporta un atteggiamento aperto ma critico, orientato a sondare non solo la necessità ed auspicabilità di risposte normative e di governo, di principi di legalità dell'amministrazione artificiale (si sarebbe detto di legalità algoritmica, finora), ma le condizioni della loro effettiva percorribilità.

Provando a testare le soluzioni in campo, ma anche a ragionare su quali percorsi possano rendere effettive le esigenze di tutela del cittadino: un cittadino che da un lato deve poter beneficiare dei miglioramenti legati all'ingresso dei nuovi strumenti e delle nuove soluzioni, ma dall'altro non può vedere arretrare significativamente i meccanismi di garanzia dei propri diritti ed interessi per ragioni di evoluzione tecnologica. Lo sviluppo della tecnica va quindi sempre accompagnato dalla ricerca di una legalità adeguata alle nuove forme, tecnologiche e sociali.

Questa legalità andrà costruita ritornando sui principi (certo di trasparenza, non esclusività, non discriminazione), ma riflettendo a fondo sulle condizioni che li rendono effettivi. E cercando di elaborare risposte secondo coordinate che sono da costruire ma rispetto alle quali si avvertono alcune tendenze.

La prima: parte della tutela si sposta dal procedimento all'organizzazione, dal momento di esercizio del potere alle condizioni organizzative del suo esercizio (quali uffici, come attrezzati, in che misura capaci di utilizzare i propri strumenti) ed alle

stesse caratteristiche intrinseche della "macchina" (in quanto essa stessa "trasparente", "affidabile"). È questa la direzione che d'altra parte ci suggerisce l'AI Act europeo. La tutela dell'individuo deve entrare di design nei prodotti e nei processi: è questa d'altra parte una direzione già tracciata da numerose regolazioni, prima tra tutte quella di protezione dei dati personali (che un ruolo così importante ha svolto nella costruzione della stessa legalità algoritmica).

La seconda: la questione va colta non in termini assoluti, ma con un approccio che sia anche pragmatico e orientato al rischio. L'amministrazione artificiale non è applicabile in tutti i contesti, ma va considerata come un potere da esercitare in quanto necessario ed in termini di proporzionalità, tenuto conto dei diritti coi quali si confronta e ai quali deve dare soddisfazione. In questi termini si può ipotizzare la regola di tendenziale preferibilità per soluzioni (solo) "algoritmiche", ma non bisogna neppure sottovalutare i limiti delle decisioni algoritmiche proprio in quanto "rigidamente" pre-ordinate.

La terza: questo potere va esercitato in trasparenza. Una trasparenza che non assume le forme della piena *explainability* ma deve mutare per continuare ad offrire adeguate garanzie: una trasparenza forse più debole, ma plurale, in grado di illuminare le scelte di utilizzo di questo potere, valorizzando forse maggiormente la prospettiva della trasparenza come controllo diffuso (su scelte organizzative, sulle soluzioni adottate) rispetto ad una trasparenza di tutela del singolo coinvolto nello specifico atto di esercizio del potere. Il mantenimento della quale appare necessaria, anche per una prospettiva di controllo giurisdizionale come ben evidenzia Napoli³⁴, ma va costruita.

La quarta: la capacità dell'amministrazione di non essere catturata dalle macchine, e di fornire risposte all'individuo di fronte alle decisioni automatizzate frutto di AI, dipende in misura non secondaria dalla qualità dell'amministrazioni e dalla ricchezza di competenze di cui dispone³⁵. L'amministrazione artificiale richiede capacità di alto livello, non riducibili a "semplici" questioni di riqualificazione del personale: deve disporre di

33. "Come imparare a smettere di preoccuparsi e accogliere il futuro con l'immaginazione" è appunto il titolo di un paragrafo del volume di LEE-QIUFAN 2023, p. 17.

34. Cfr., in questa sezione della Rivista, NAPOLI 2024.

35. Diffusamente v. sul punto FALCONE 2024, in questa sezione della Rivista. Sollecitazioni in questa direzione già in DI MASCIO-NATALINI 2023; AIPDA 2020.

AI Talent, come ci mostra la strategia statunitense³⁶. La nuova amministrazione artificiale ha uno straordinario bisogno di capacità alte ed interdisciplinari, che devono rivolgersi all'ottimizzazione delle strategie di utilizzo, al controllo dell'algoritmo, ma anche alla costruzione di AI pubbliche o comunque pensate coerentemente con i caratteri e le missioni costituzionali delle amministrazioni, nuovi algoritmi in grado di disvelarsi e disvelare il potere computazionale³⁷. Non può non colpire negativamente, in questa prospettiva, la scelta del ddl governativo sulle AI di impostare la nuova politica secondo il criterio di invarianza di spesa.

La quinta: all'avvio del percorso abbiamo solo alcune delle risposte di cui abbiamo bisogno. La strategia di regolazione dell'ingresso di soluzioni di AI va affrontata anche nel percorso. I primi commenti alla politica americana esplicitata dall'*Executive order* Biden n. 14110³⁸ hanno evidenziato l'importanza ed opportunità di un approccio pragmatico, di costruzione di centri di competenza, orientato al rischio e alla definizione graduale di soluzioni spesso da adattare ai singoli casi. Non c'è un sentiero, viandante, il sentiero si fa camminando³⁹.

Riferimenti bibliografici

- AIPDA (2020), *Annuario 2019. Quali saperi servono alla pubblica amministrazione? Selezione, valorizzazione e tutela della professionalità pubblica*, Editoriale Scientifica, 2020
- S. ARDUINI (2021), *La scatola nera della decisione giudiziaria: tra giudizio umano e giudizio algoritmico*, in "BioLaw Journal – Rivista di BioDiritto", 2021, n. 2
- G. AVANZINI (2019), *Decisioni amministrative e algoritmi informatici*, Editoriale Scientifica, 2019
- C. BARBATI (2021), *La decisione pubblica al cospetto della complessità: il cambiamento necessario*, in "Diritto pubblico", 2021, n. 1
- Y. BATHAEE (2018), *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, in "Harvard Journal of Law & Technology", vol. 31, 2018, n. 2
- E. BELISARIO, G. CASSANO (a cura di) (2023), *Intelligenza artificiale per la pubblica amministrazione*, Pacini, 2023
- K. BOUSMALIS, G. VEZZANI, D. RAO et al. (2023), *RoboCat: A Self-Improving Foundation Agent for Robotic Manipulation*, June 2023
- V. BRIGANTE (2019), *Evolving Pathways of Administrative Decisions*, Editoriale Scientifica, 2019
- E. CARLONI (2024), *Il sentiero si fa camminando: la strategia statunitense per intelligenze artificiali sicure ed affidabili. Commento all'Executive Order 14110 on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, in "Giornale di diritto amministrativo", 2024, n. 1
- E. CARLONI (2024-A), *Transparency within Artificial Administration. Principles, Paths, Perspectives and Problems*, in "Italian Journal of Public Law", vol. 16, 2024, n. 1
- E. CARLONI (2023), *La trasparenza amministrativa e gli algoritmi*, in E. Belisario, G. Cassano (a cura di), "Intelligenza artificiale per la pubblica amministrazione. Principi e regole del procedimento amministrativo algoritmico", Pacini, 2023

36. Si v. l'*Executive order* 14110 di Biden, on *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, per il quale si rinvia a CARLONI 2024.

37. Spunti in PONTI 2024; cfr., per es., COGLIANESE-LAI 2022.

38. Cfr. COGLIANESE 2024; CARLONI 2024, p. 135 ss.

39. Il richiamo è al noto passo di Antonio Machado: «Caminante, no hay camino, se hace camino al andar» (Campos de Castilla, 1912); una affermazione molto simile è attribuita anche a Franz Kafka («il cammino si costruisce viaggiando»).

- E. CARLONI (2020), *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in “Diritto Amministrativo”, 2020, n. 2
- E. CARLONI (2019), *Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni*, in “Diritto pubblico”, 2019, n. 2
- G. CARULLO (2023), *Piattaforme digitali e interconnessione informativa nel nuovo Codice dei Contratti Pubblici*, in “federalismi.it”, 2023, n. 19
- R. CAVALLO PERIN (2020), *Ragionando come se la digitalizzazione fosse data*, in “Diritto amministrativo”, 2020, n. 2
- R. CAVALLO PERIN, I. ALBERTI (2020), *Atti e procedimenti amministrativi digitali*, in R. Cavallo Perin, D.-U. Galetta, “Il diritto dell’amministrazione pubblica digitale”, Giappichelli, 2020
- R. CAVALLO PERIN, D.-U. GALETTA (a cura di) (2020), *Il diritto dell’amministrazione pubblica digitale*, Giappichelli, 2020
- R. CAVALLO PERIN, M. LIPARI, G.M. RACCA (a cura di) (2024), *Contratti pubblici e innovazioni nel nuovo Codice. Trasformazioni sostanziali e processuali*, Jovene, 2024
- A. CERRILLO MARTINEZ, J. PONCE SOLE (a cura di) (2024), *Artificial intelligence in public administration in light of the AI Act*, European Public Law Series, 2024
- S. CIVITARESE MATTEUCCI (2019), *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità*, in “Diritto pubblico”, 2019, n. 1
- C. COGLIANESE (2024), *A People-and-Processes Approach to AI Governance*, in “The Regulatory Review”, January 2024
- C. COGLIANESE, A. LAI (2022), *Algorithm vs. Algorithm*, in “Duke Law Journal”, vol. 71, 2022, n. 6
- K. CRAWFORD (2021), *Né intelligente né artificiale. Il lato oscuro dell’IA*, il Mulino, 2021
- M. DE DONNO, F. DI LASCIO (a cura di) (2022), *Public Authorities and Complexity. An Italian Overview*, Edizioni Scientifiche Italiane, 2022
- F. DI MASCIÒ, A. NATALINI (2023), *La capacità amministrativa e il PNRR*, in “Giornale di diritto amministrativo”, 2023, n. 4
- M. EBERS (2020), *Regulating AI and Robotics: Ethical and Legal Challenges*, in M. Ebers, S. Navas (eds.), “Algorithms and Law”, Cambridge University Press, 2020
- M. FALCONE (2024), *La data science come nuovo sapere per governare le intelligenze artificiali nelle pubbliche amministrazioni*, in “Rivista italiana di informatica e diritto”, 2024, n. 2
- M. FALCONE (2023), *Ripensare il potere conoscitivo pubblico tra algoritmi e Big Data*, Editoriale Scientifica, 2023
- E. FALLETTI (2020), *Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche*, in “Il Diritto dell’informazione e dell’informatica”, 2020, n. 2
- L. FEI FEI (2024), *Tutti i mondi che vedo. Curiosità, scoperta e meraviglia all’alba dell’intelligenza artificiale*, LUISS, 2024
- L. FEI FEI, J. ETCHEMENDY (2023), *Why the U.S. Needs a Moonshot Mentality for AI — Led by the Public Sector*, in “Wall Street Journal”, 9 December 2023
- G. FINOCCHIARO (2024), *Intelligenza artificiale. Quali regole?*, il Mulino, 2024
- L. FLORIDI (2022), *Etica dell’intelligenza artificiale. Sviluppi, opportunità, sfide*, Raffaello Cortina Editore, 2022

- I. FORGIONE (2024), *La prospettiva dell'intelligenza artificiale nel procedimento e nell'attività amministrativa*, in "Rivista italiana di informatica e diritto", 2024, n. 2
- D.-U. GALETTA (2023), *Human-stupidity-in-the-loop? Riflessioni (di un giurista) sulle potenzialità e i rischi, dell'Intelligenza Artificiale*, in "Federalismi.it", 2023, n. 5
- D.-U. GALETTA (2022), *Transizione digitale e diritto ad una buona amministrazione: fra prospettive aperte per le Pubbliche Amministrazioni dal Piano Nazionale di Ripresa e Resilienza e problemi ancora da affrontare*, in "federalismi.it", 2022, n. 7
- G. GALLONE (2023), *Riserva di umanità e funzioni amministrative*, Cedam, 2023
- F. GIANNOTTI, D. PEDRESCHI (2019), *«Explainable AI». Aprire le scatole nere per una Intelligenza Artificiale (AI) umana*, in "Gnosis", 2019, n. 2
- A. LALLI (a cura di) (2024), *La regolazione pubblica delle tecnologie digitali e dell'intelligenza artificiale*, Giappichelli, 2024
- K.F. LEE, C. QIUFAN (2023), *Scenari dal futuro dell'intelligenza artificiale*, LUISS, 2023
- E. LONGO (2022), *I processi decisionali automatizzati e il diritto alla spiegazione*, in A. Pajno, D. Donati, A. Perrucci (a cura di), "Intelligenza artificiale e diritto: una rivoluzione?", vol. I, il Mulino, 2022
- B. MARCHETTI (2022), *Amministrazione digitale*, in "Enciclopedia giuridica – I Tematici, Funzioni amministrative", Giuffrè, 2022
- B. MARCHETTI (2021), *La garanzia dello human in the loop alla prova della decisione amministrativa algoritmica*, in "BioLaw Journal - Rivista di BioDiritto", 2021, n. 2
- D. MARTIRE (2024), *Human in the loop. L'essere umano come fattore condizionante della – o condizionato dalla – intelligenza artificiale*, in "Rivista italiana di informatica e diritto", 2024, n. 2
- B.G. MATTARELLA, B. MARCHETTI (2024), *La digitalizzazione dei contratti pubblici nel nuovo codice*, Giappichelli, 2024
- C. NAPOLI (2024), *Strumenti informatici nel processo decisionale amministrativo ed effettività del diritto di difesa: questioni vecchie e problemi nuovi alla luce del Regolamento (UE) 2024/1689*, in "Rivista italiana di informatica e diritto", 2024, n. 2
- C. NAPOLI (2020), *Algoritmi, Intelligenza Artificiale e formazione della volontà pubblica: la decisione amministrativa e quella giudiziaria*, in "Rivista AIC", 2020, n. 3
- A. NATALINI (2006), *Il tempo delle riforme amministrative*, il Mulino, 2006
- P. PIRAS (2020), *Il tortuoso cammino verso un'amministrazione nativa digitale*, in "Il Diritto dell'informazione e dell'informatica", n. 1, 2020
- B. PONTI (2024), *Il fornitore dell'algoritmo quale soggetto estraneo all'amministrazione*, in "Rivista italiana di informatica e diritto", 2024, n. 2
- B. PONTI (2023), *Tre scenari di digitalizzazione amministrativa "complessa": dalla interoperabilità predicata alla standardizzazione praticata*, in "Istituzioni del Federalismo", 2023, n. 3
- B. PONTI (2022), *Le diverse declinazioni della 'Buona amministrazione' nel PNRR*, in "Istituzioni del Federalismo", 2022, n. 2
- L. PREVITI (2022), *La decisione amministrativa robotica*, Editoriale Scientifica, 2022
- G.M. RACCA (2023), *Trasformazioni e innovazioni digitali nella riforma dei contratti pubblici*, in "Diritto amministrativo", 2023, n. 4
- S. RODOTÀ (2009), *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, 2009

- C.P. SANTACROCE (2023), *PNRR, "riforma orizzontale" della pubblica amministrazione e disciplina generale del procedimento amministrativo*, in "Il diritto dell'economia", 2023, n. 1
- A. SAPORITO (2023), *Verso una "nuova" amministrazione digitale*, in "Ambientediritto.it", 2023, n. 2
- G. SGUEO (2022), *Il divario: I servizi pubblici digitali tra aspettative e realtà*, Egea, 2022
- A. SIMONCINI (2019), *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in "BioLaw Journal - Rivista di BioDiritto", 2019, n. 1
- L. TORCHIA (2023), *Lo Stato digitale. Una introduzione*, il Mulino, 2023



DARIO MARTIRE

Human in the loop. L'essere umano come fattore condizionante della – o condizionato dalla – intelligenza artificiale

Il recente dibattito ha evidenziato il legame tra le identità virtuali, sviluppatesi con il digitale e l'intelligenza artificiale, e i concetti giuridici su cui si basa la giuspubblicistica. Queste sfide, seppur già presenti, sono state accentuate dall'intelligenza artificiale. "Human in the loop" (HITL) indica un approccio in cui l'essere umano è coinvolto nel ciclo di addestramento e test degli algoritmi, mantenendo un ruolo centrale nei processi decisionali. Tuttavia, il termine "loop" può anche significare "cappio" e descrivere un essere umano intrappolato in un ciclo ripetitivo e chiuso. L'essere umano può quindi essere visto sia come un fattore condizionante che condizionato dall'intelligenza artificiale, con implicazioni significative per la coscienza di sé e l'identità. Questa dicotomia offre una prospettiva di ricerca sull'essere umano e il rapporto tra essere e dover essere costituzionale.

Stato costituzionale – Intelligenza artificiale – Algoritmo – Democrazia

Human in the loop. The human being as a conditioning factor of – or conditioned by – artificial intelligence

The recent debate has highlighted the link between virtual identities, which have developed with digital and artificial intelligence, and the legal concepts on which jurisprudence is based. These challenges, while already present, have been accentuated by artificial intelligence. "Human in the loop" (HITL) denotes an approach in which humans are involved in the cycle of training and testing algorithms while maintaining a central role in decision-making processes. However, the term "loop" can also mean "noose" and describe a human being trapped in a repetitive, closed loop. The human being can thus be seen as both conditioning and being conditioned by artificial intelligence, with significant implications for self-awareness and identity. This dichotomy offers a research perspective on human being and the relationship between "is" and "ought".

Constitutional State – Artificial intelligence – Algorithm – Democracy

L'Autore è ricercatore di tipo B di Istituzioni di diritto pubblico presso Sapienza – Università di Roma

Questo contributo fa parte della sezione monografica *Cittadini e pubbliche amministrazioni tra AI e diritto all'umano*, a cura di Enrico Carloni

1. In un recente dibattito sul futuro del diritto pubblico si è messo a fuoco il legame tra la dimensione virtuale dell'esistenza e dell'identità – provocata dallo sviluppo del digitale e, soprattutto, dell'intelligenza artificiale – e la matrice dei relativi concetti artificiali su cui, come è noto, si è foggata la giurispubblicistica¹. Sfide e problematiche che, peraltro, erano già visibili in passato, ma che, tuttavia, lo sviluppo dell'intelligenza artificiale ha, quantomeno, accentuato.

L'espressione "Human in the loop", letteralmente l'uomo nell'anello, o ancora più precisamente l'uomo nel circuito, è stata ed è ancora utilizzata per indicare, in estrema sintesi, un approccio in cui l'essere umano risulta coinvolto nel ciclo di addestramento, messa a punto e test dell'algoritmo. Un modello, dunque, che richiede una costante interazione dell'uomo con la macchina intelligente e che si declina sulla base dell'imperativo per cui l'essere umano deve mantenere il ruolo di protagonista all'interno dei processi decisionali. Protagonismo che evidentemente presuppone una libera scelta, inevitabilmente legata alla coscienza di sé, attribuito cruciale dell'identità.

Loop, come è noto, non significa tuttavia solo anello o circuito, una catena al cui interno è inserito l'essere umano, ma anche cappio o nodo. Se da un lato, dunque, si cerca di attribuire all'essere umano una posizione centrale ed essenziale all'interno di un processo e di ricondurre, dunque, la macchina e il suo prodotto all'autodeterminazione della persona umana, dall'altro, si scopre, al contrario, la possibilità concreta che esso risulti prigioniero e, in una prospettiva digitale, "in loop", intrappolato all'interno di un ciclo chiuso e ripetitivo che influenza significativamente la sua esistenza e dal quale risulta complesso, se non impossibile, riuscire a liberarsi.

Un essere umano, allora, rappresentato alternativamente come fattore condizionante della – o condizionato dalla – intelligenza artificiale. Una duplice possibilità che ne rivela la fecondità euristica: una ricerca orientata alla scoperta dell'essere umano, alla luce del rapporto tra essere e dover essere, che intreccia inoltre vari temi, peraltro trasversali, e che presuppone necessariamente il confronto con altri studi.

Concentrandoci solo per un attimo su quest'ultimo profilo, risulta interessante e proficuo un aneddoto verificatosi in Assemblea costituente. Nel dibattito su quello che sarebbe poi divenuto l'art. 7 della Costituzione, Vittorio Emanuele Orlando affermava: «E passiamo a quest'altra definizione — qui mi avvicino ad una zona infiammabile: — "Lo Stato e la Chiesa cattolica sono, ciascuno nel proprio ordine, indipendenti e sovrani". Badate, questa definizione io l'accoglierei; però, non come deputato che fa una Costituzione, bensì come un cultore di diritto. Da un punto di vista, diciamo, di studio, di speculazioni teoriche, io mi accosto effettivamente a questa teoria. Ma perché metterla nella Costituzione, dando luogo ad equivoci, ad interpretazioni, che potrebbero essere false ed erronee per chi non si è, direi, specializzato in questo genere di studi? Si può essere una persona coltissima, eppure ignorare o non capire una qualche cosa. Io non ho mai capito la dottrina di Einstein, per quanto l'abbia studiata. E così via»². Per il positivismo orlandiano la scienza giuridica era in un certo senso autoreferenziale, si basava esclusivamente su se stessa; non stupisce dunque che la dottrina di Einstein non fosse neanche da esplorare. Indagare il tema dell'intelligenza artificiale e le problematiche che essa pone rispetto ai principi costituzionali impone, al contrario, il confronto con le altre scienze. La nostra Costituzione

1. AA.VV. 2024.

2. Cfr. la seduta del 10 marzo 1947, Assemblea Costituente, in www.nascitacostituzione.it.

ne fornisce d'altronde la migliore prova empirica, avendo prodotto in coloro che l'hanno letta e che l'hanno vissuta una crescita non solo giuridica ma anche, e soprattutto, culturale.

Tornando alla questione, è necessario fornire alcune coordinate prima di addentrarsi nella sostanza. Con la parola "robot" si intende un automa, un operatore meccanico automatico controllato da un cervello elettronico, con particolare riferimento agli apparecchi programmabili usati in alcuni settori dell'industria e della ricerca scientifica per operazioni seriali e in automatico. Un artificio, dunque, opera dell'uomo evidentemente, che tuttavia incontra, a un certo punto del Novecento, un altro artificio, la c.d. intelligenza artificiale, che incide, o dovrebbe incidere, sulla capacità di questo robot di autonomizzarsi non solo nella parte meccanica, ma anche e soprattutto nella parte intellettuale o, potremmo dire, spirituale.

Il termine "intelligenza artificiale", come è noto, è stato coniato nel 1956 da un informatico per descrivere un'attività posta in essere dalle macchine con metodo analogo a quella realizzata dagli esseri umani. Nel corso del tempo gli informatici e i filosofi della mente si sono interrogati sui concetti di intelligenza e sulle relative differenze; sono state elaborate le nozioni di intelligenza artificiale forte e debole³, le tesi c.d. funzionaliste e connessioniste⁴.

La questione principale oggi, tuttavia, concerne più che altro l'interruzione di quel percorso che aveva portato gli sviluppatori dell'intelligenza artificiale verso la pressoché totale sovrapposizione tra intelligenza umana e artificiale. In altri termini, attualmente l'evoluzione non si dirige più verso l'imitazione dell'intelligenza umana, bensì verso una strada autonoma, scevra dai meccanismi propri della logica deduttiva, per accogliere, al contrario, meccanismi basati su sistemi prettamente induttivi e che privilegiano la statistica.

In una prospettiva costituzionalistica, ciò incide da un lato sulla questione dei processi, intesi come attività e forme mediante le quali organi a ciò deputati esercitano, diciamo genericamente, un potere, che può essere politico, di amministrazione, di giurisdizione e che presuppone, sul piano logico, un modo di procedere ordinato in relazione a un determinato fine.

In secondo luogo, assume una rilevanza inedita la capacità persuasiva, oramai acclarata, dell'intelligenza artificiale, in grado di condizionare l'autonoma determinazione dell'essere umano e, indirettamente, di incidere significativamente su alcune conquiste del costituzionalismo.

In entrambi i casi, a mio avviso l'intelligenza artificiale presenta problemi in parte già noti, ma con una carica espansiva evidentemente sconosciuta. Basti pensare all'obiettivo dichiarato dai creatori e, più in generale, dai sostenitori di questi strumenti, di garantire prevedibilità e predittività e, dunque, anticipazione e previsione di determinati eventi; obiettivo ammirevole che, tuttavia, cela il prezzo che potrebbe pagarsi in merito all'autonomia cognitiva della persona e del cittadino, nonché alla discrezionalità dell'autorità – anche quella garante dei diritti – nell'esercizio del potere.

2. Ragionare in termini di essere umano condizionato e di limitazione o annullamento della sua libertà di autodeterminazione innesta alcune riflessioni sulla natura (anche giuridica) dell'uomo che storicamente ne è stato privato.

Per Aristotele lo schiavo è un essere intermedio e imperfetto mentre l'uomo libero e riuscito è quello che, avendo pienezza virtuale del *logos*, pensiero e parola, ed essendo in grado di discorrere secondo ragione, è dunque capace di autogoverno, di prendere decisioni preveggenti, perché possiede la c.d. *proairesis*, è in grado di andare verso un fine⁵.

3. Per i sostenitori della IA forte le macchine potranno mostrare una intelligenza analoga a quella umana. All'opposto, coloro che sostengono la tesi della IA debole ritengono che i computer non potranno mai replicarla.

4. Per i funzionalisti, di cui Putnam è stato probabilmente il maggior esponente, la mente umana può essere descritta come una serie di stati mentali basati sulla loro funzione, per cui il cervello funzionerebbe proprio come una macchina elaborata. Il connessionismo ricostruisce la mente come qualcosa di diverso da un software, in quanto avente connessioni neurali, che si allacciano con gli stimoli esterni e con la memoria, impossibile da formalizzare negli algoritmi.

5. Questo aspetto della prevedibilità ritornerà, sia con riferimento alla macchina dotata di intelligenza artificiale, sia con riferimento alla certezza giuridica e all'essere umano immerso nella società di oggi. Su tale aspetto cfr. BODEI 2019.

Lo schiavo è dunque un ente situato tra la cosa e la persona, tra lo spirito e il corpo, e, non essendo in grado di autogovernarsi, non può comandare e comandarsi, ma solo ubbidire; tale relazione imposta sulla obbedienza instaura allora una sorta di simbiosi con il padrone, di cui lo schiavo comprende solo gli ordini.

Si potrebbe sintetizzare così: da un lato, mancanza di previsione dell'agire rispetto a un fine prestabilito, dall'altro, incapacità di comprensione dello stato di soggezione e di dipendenza non solo fisico, ma soprattutto psicologico e anche in un certo senso affettivo e spirituale.

Accostare tale idea alle macchine e all'intelligenza artificiale significa allora interrogarsi sulla coscienza e, passando al piano giuridico, sulla possibile configurazione di una sorta di *habeas mentem* o *habeas animam*, di una libertà di pensare presupposto, dunque, di tutte le altre libertà e scevra, per quanto possibile, da condizionamenti esterni o, quantomeno, da alcuni condizionamenti esterni. Provare a immaginare dunque un'area inaccessibile, o, quantomeno, un pensiero condizionato esternamente solo da fattori socialmente accettabili.

Nella dinamica schiavo-padrone, il primo finiva per rispecchiarsi nel secondo e viceversa, in una sorta di reciproco riconoscimento che contribuiva a determinare le loro rispettive identità inserite all'interno di una determinata gerarchia sociale. Tuttavia, anche una volta formalmente eliminata, si è ipotizzato che gli esseri umani, divenuti formalmente liberi, potessero ancora essere rappresentati come enti condizionati dall'altro da sé, dai bisogni costruiti e indotti da una società caratterizzata, in ogni suo settore, dalle regole autonome del mercato, inteso nel senso più ampio possibile. Per alcuni, peraltro, questi condizionamenti sarebbero stati talmente invasivi da qualificare gli esseri umani ancora, sostanzialmente, come schiavi⁶.

Non che prima l'essere umano non fosse dominato dai propri desideri: è noto come per Spinoza l'uomo creda, si illuda, di essere lui a scegliere cosa desiderare, ma i desideri in realtà non sono scelte, sono frutto del *conatus*. Il desiderio nasce allora dall'istinto all'autoconservazione e, dunque, il condizionamento è, per certi versi, connaturato

alla sua essenza, ma risulta, proprio per questo, socialmente e giuridicamente accettabile.

Nell'idea di essere umano dominato dai bisogni dettati da una società di mercato, consumistica, invece, continua ad esserci, seppur diversa, l'idea, stavolta inaccettabile, di uno stato di soggezione, di una soggettività limitata di fatto, ancora caratterizzata da desideri da altro determinati. Una etero-determinazione che però ha un elemento in più, poiché è sottaciuta da colui o da ciò che lo determina e risulta difficilmente afferrabile da colui che è determinato. Da una schiavitù formale e limitata nei destinatari ad una schiavitù sostanziale (perché formalmente inesistente) e generalizzata, che, come tale, deve essere svelata e contrastata.

Questa lettura può essere feconda anche oggi, nell'analisi di questi nuovi strumenti tecnologici, artificialmente intelligenti, che incidono sul rapporto che l'essere umano ha con se stesso – sulla questione della coscienza e dell'identità – che ridonda poi anche nella questione dell'identità costituzionale, e, dall'altro e di riflesso, nel rapporto che si instaura con un potere che si presenta diverso, in quanto avente, sotto certi profili, meno confini e maggiore capacità di mascherare i suoi intenti.

Per certi versi, dunque, l'intelligenza artificiale pone dei problemi già noti al costituzionalismo, che potremmo riassumere nella questione della soggettività e della disuguaglianza, ma con una forza più incisiva; al tempo stesso pone nuovi rischi, determinati dalla capacità di intromettersi nell'animo umano, nella psiche, in violazione del foro tradizionalmente definito come interno, spazio che si pensava inaccessibile e che, dunque, ci riporta agli albori del costituzionalismo.

Sempre in questa prospettiva, volgendo per un istante lo sguardo al passato, è a partire dal Cinquecento che si afferma quel legame tra matematica come scienza teorica, proprio perché essa sola dà certezza, che diviene modello per la riforma del pensiero – basti pensare al Discorso sul metodo di Cartesio e al metodo scientifico di Galilei, secondo il quale il sapere può solo fondarsi sulle “sensate esperienze” (metodo empirico) e sulle “necessarie dimostrazioni” (metodo logico-matematico) – e quella che è la sua affermazione sociale. Un

6. È noto come, a partire dai *Manoscritti economico-filosofici* del 1844 di Marx, il tema dell'alienazione si sia sposato con quello della sfera economica della produzione materiale.

forte legame, dunque, tra matematica, certezza e costumi sociali, anche e soprattutto commerciali, espressione di quella esigenza di prevedibilità che sarà tradotta più avanti, dalla scienza giuridica, nei codici, tipica espressione della mentalità borghese.

Non a caso, prevedibilità, stabilità, astrattezza e certezza saranno caratteristiche tipiche dello Stato moderno, ove saranno assunte a valori fondanti dell'ordine giuridico.

Tornando ad oggi, infatti, e provando a trarre delle prime conclusioni in ordine alle problematiche che l'intelligenza artificiale pone rispetto ai rapporti tra i poteri dello Stato che, come è noto, ridonda inevitabilmente anche sulla garanzia dei diritti fondamentali, secondo prospettive già indagate anche tra i costituzionalisti, «il giudice-matematico o geometra è quello che più si avvicina all'idea della formalizzazione della giurisprudenza e all'ideale della scienza del diritto come scienza esatta, con quel che segue quanto a prevedibilità, stabilità, certezza delle sue soluzioni: un ideale effettivamente coltivato, soprattutto dal razionalismo giuridico del Seicento e del Settecento di cui il positivismo giuridico legalistico, quanto al metodo, si pone come legittimo erede»⁷.

La questione del giudice robot automa – che si serve anche dell'intelligenza artificiale – pone dunque problematiche già indagate dal costituzionalismo. Parte della dottrina l'ha utilizzata per mettere in discussione ancora una volta alcune teorie dell'interpretazione e una concezione della giurisdizione che avrebbe generato una grave incertezza in danno dei consociati e un significativo spostamento di potere in favore della magistratura, al prezzo di un serio indebolimento della sua

legittimazione sistemica, concludendo, tuttavia, per la preferenza, in ogni caso, del giudice umano⁸.

Altra parte della dottrina ha evidenziato, al contrario, come attraverso gli algoritmi si ripresenti l'idea di un giudice-funzionario bocca della legge. Il riferimento alla matematica, scienza deduttiva per eccellenza, come modello della giurisprudenza che esalta la prevedibilità, è infatti denso di significato, proprio perché caratteristica apprezzata soprattutto dai poteri privati che operano nel mercato⁹.

Il risultato dell'algoritmo è il prodotto inevitabile di dati confezionati in un dato momento storico, potremmo dire che è garante di una stabilità senza tempo, come si concepiva allora il diritto pubblico, ove dunque il futuro era irrilevante. Il risultato che ne scaturisce può allora costituire forse la migliore risposta in termini di efficienza e razionalità, ma presenta inevitabilmente almeno gli stessi limiti della legge generale e astratta confezionata in modo rigido, non lasciando spazi di manovra sufficienti per la modulazione delle conseguenze che, in base alla valutazione di fatti socialmente rilevanti, anche successivi ai dati immessi nell'algoritmo, si verificano e, specialmente nell'interpretazione (anche costituzionale), non possono non acquisire rilevanza. In altri termini, la decisione algoritmica, pur presentandosi come *razionale*, può del pari risultare *non ragionevole*.

Peraltro, come si diceva all'inizio, l'intelligenza artificiale oramai si basa più su metodi induttivi e sulla statistica, con tutti i limiti che ne conseguono anche in termini di efficienza e razionalità¹⁰. Si potrebbe sostenere che la validità dell'induzione non sia basata sulla sua validità logica (come sosteneva Aristotele), né sulla sua conformità alla

7. ZAGREBELSKY-MARCENÒ 2018, p. 97. Secondo LUCIANI 2018, p. 875 ss., sostituire il giudice con un robot potrebbe, solo in teoria, garantire certezza giuridica: «L'esigenza oggettiva di certezza, con il suo connesso profilo soggettivo dell'affidamento, si colloca autenticamente al centro degli ordinamenti contemporanei. Sulla scia di Weber, Natalino Irti l'ha collegata allo sviluppo del capitalismo, mettendo in rilievo che un mondo prevedibile è essenziale per l'imprenditore e le sue strategie di investimento, ma a me sembra che il rilievo weberiano, per quanto ineccepibile, sia solo parziale e che quell'esigenza sia, più in generale, un lascito della modernità, la quale, se comprende il capitalismo, nel capitalismo non si esaurisce. Un lascito della modernità soprattutto politica, nel senso che lo Stato moderno nasce (nel disastro delle guerre civili e di religione) come erogatore di prestazioni di sicurezza (fisica) per i sudditi e che la certezza giuridica non è altro che la proiezione della sicurezza nel dominio del diritto. Statualità sicurezza e certezza sono, dunque, una triade politica indissolubile, la cui costruzione precede di un paio di secoli i trionfi economici del capitalismo». Cfr. IRTI 2017, p. 21 ss.

8. LUCIANI 2018, p. 892 ss.

9. Sia consentito rinviare a MARTIRE 2022.

10. Si potrebbe far riferimento a Russell e al suo tacchino e ovviamente a Popper.

natura della mente umana (come sosteneva David Hume), ma sulla *verità comune* (come già sosteneva probabilmente il Socrate di Platone), che si sviluppa nel tempo e che risponde alle domande poste da una specifica comunità umana, elemento ancor più prezioso per la scienza giuridica. Tuttavia, trattandosi di scienza applicata poi al mondo del diritto, il problema, per certi versi, rimarrebbe.

Il dover essere, *in primis* quello costituzionale, si propone, d'altro canto, l'obiettivo di modificare la realtà in una prospettiva orientata al futuro, venendo alla luce con lo scopo di condizionare il contesto sociale in vista del raggiungimento di principi costituzionali. Basti pensare alla enfatica aspirazione all'eternità di tali documenti¹¹.

Il diritto costituzionale, secondo tale ottica, accoglie profili sostanziali (pensiamo all'art. 3 Cost.), proprio perché costituisce, potremmo dire, il diritto del caso particolare, che rifiuta le idee ricevute dall'Illuminismo giuridico relative alle norme giuridiche perfette in quanto chiare, semplici e uniformi, e, in tale prospettiva, razionali, per accogliere, al contrario, un ordinamento in cui gli automatismi – per quanto pregni di razionalità – vengono sanzionati per far spazio alla ragionevolezza, perseguita, a scapito della regola normativa automatica, mediante l'attribuzione di discrezionalità al giudice, unico soggetto in grado di cogliere le diverse sfumature del caso concreto, che conduce all'applicazione di una regola diversa rispetto a quella generale, predeterminata, ma anche prevedibile¹².

3. Recentemente, in un convegno dedicato alla privacy e ai c.d. neurodiritti, il Presidente del Garante per la protezione dei dati personali, Pasquale Stanzone, ha affermato che «è almeno a partire da Cartesio che l'identità, la soggettività, la stessa differenza dell'uomo (come singolo e come specie) viene identificata nel pensiero – il *cogito ergo sum* –, la cui proiezione organica è il cervello: limite

invalicabile persino per il più coercitivo e totalitario dei poteri (che pur avesse tentato di orchestrare consensi e costruire culture), proprio perché correlato neurale della coscienza»¹³.

Il dualismo cartesiano mente-corpo assume una certa rilevanza per lo studio dell'intelligenza artificiale, perché la suddivisione di due diverse sostanze, l'una, immateriale, intesa come pensiero libero e volontario tipicamente dell'uomo, l'altra, materiale, intesa come corpo meccanico dotato di estensione, implica una concezione del corpo come una mera macchina guidata dalla mente, mentre le passioni derivano dall'esterno e l'uomo è in grado di controllarle senza esserne schiavo.

Non a caso Cartesio è significativo, tra le tante cose, per aver dato alle macchine, avendone constatata l'effettiva autonomia nel funzionamento e certa complessità e variabilità nella organizzazione, la dignità di oggetto del pensiero, sia per motivi storici che filosofici.

D'altra parte, era stato lo stesso Cartesio a mettere in dubbio tutte le conoscenze, a partire da quelle sensibili. Per trovare la base solida del metodo aveva messo in dubbio tutto, ma prima di tutto i sensi, in quanto, non potendo essere certi che la realtà che percepiamo sia vera, tutto potrebbe essere un inganno. Le conoscenze sensibili non potevano dunque essere poste a fondamento del metodo, perché i sensi non superavano il test del dubbio.

Si è peraltro sostenuto come la scienza giuridica occidentale sia basata sul presupposto agostiniano del foro interiore¹⁴, per cui, a differenza di Cartesio, l'essere umano non è solo mente, puro Cogito, ma mente-cuore, ragione-passione. La lingua, si è detto, è la prima tecnologia, ma, al tempo stesso, anche la prima forma di potere¹⁵.

Damasio, noto neurologo e neuroscienziato, ha fortemente criticato questa idea cartesiana; il suo volume "L'errore di Cartesio" invita a sbarazzarsi del dualismo mente-corpo e, non a caso, riprende

11. Cfr. *ex multis*, LONGO 2016.

12. Cfr. SIMONCINI 2019, p. 77 ss.

13. STANZIONE 2021, p. 10.

14. MARRAMAO 2021, p. 58. A suo avviso, il foro interiore non è pura mente, ma un pensiero-corpo, un pensiero-esperienza modellato dal linguaggio, un pensiero codificato dalla parola che viene trasmessa. Pensiero tramite la lettura, condivisione tramite la diffusione. Un intimo nesso tra parola, scrittura e foro interiore. Gli studiosi di robotica lo ricondurrebbero, invece, al Cogito cartesiano, sul presupposto della mente separata dal corpo.

15. MARRAMAO 2021, p. 60.

una efficace espressione di Spinoza, secondo cui “La mente è l’idea del corpo”.

Tuttavia, non si può non rilevare come il pensiero liberale abbia avuto buon gioco nel ricondurre le libertà al dualismo cartesiano, in quanto proprio in virtù di tale presupposto il foro interno poteva essere agevolmente considerato come inaccessibile. In altri termini, più che interno e dunque inaccessibile, il foro libero risultava inaccessibile e dunque interno, perché si fondava proprio sul presupposto logico della mente separata dal corpo. In assenza di tale presupposto il potere, incidendo sul corpo, avrebbe inciso, indirettamente, anche sulla mente. Il dualismo costituiva dunque un presupposto logico utile per sostenere l’intangibilità della libertà di pensare e, a valle, per non prevedere possibili strumenti a tutela della sua eventuale violazione, proprio perché irrealizzabile.

Non a caso, sebbene nell’*Ethica* avesse teorizzato il “parallelismo” mente-corpo e, dunque, il superamento del dualismo cartesiano, anche Spinoza aveva desunto dalla libertà di pensiero tutte le altre libertà. In un passo del Capitolo XX del Trattato teologico-politico, intitolato “Si dimostra che in una libera Repubblica è lecito a chiunque di pensare quello che vuole e di dire quello che pensa”, aveva argomentato che «ciascuno è, per diritto imprescrittibile della natura, padrone dei suoi pensieri» in base alla constatazione che «per quanti risultati l’artificio abbia potuto ottenere in questo campo, tuttavia non si arrivò mai a tanto che gli uomini non sperimentassero che ognuno abbonda del proprio senso e che tanto variano le teste quanti sono i palati»¹⁶.

Ma come altri costrutti dell’ideologia liberale, anche questo si fondava su una inevitabile astrattezza, che finiva per scontrarsi con la realtà. Come è stato sostenuto, l’assunto di Spinoza che nessun artificio avrebbe potuto violare la libertà di pensare, e con essa l’irriducibile identità di ognuno, rifletteva l’epoca delle guerre di religione, nel corso della quale i tentativi di dominare le coscienze finirono con il rafforzare il sentimento della

libertà religiosa¹⁷, che, dunque, erano condizionate, seppur in una direzione opposta alla volontà del condizionante. Ma quell’assunto è tornato in discussione nei regimi totalitari, ove la propaganda dei miti politici portò gli uomini a rinunciare «al più alto privilegio umano. Essi hanno cessato di essere agenti liberi e personali. Compiendo gli stessi riti prescritti, essi cominciano a sentire, a pensare e a parlare tutti nello stesso modo»¹⁸.

I rischi di manipolazione di massa del pensiero non sono tuttavia terminati, come è noto, con il crollo dei regimi totalitari. L’uso distorto della libertà di espressione in vista della ricerca di un pubblico sempre più vasto da parte dei proprietari dei *media* televisivi, necessario alla raccolta pubblicitaria, fu segnalato anche dai nostri costituzionalisti¹⁹. Ormai «i pensieri e le notizie più diffusi tendono ad essere quelli che il pubblico gradisce: di qui una gravissima distorsione dei presupposti della libertà di manifestazione del pensiero, che viene esercitata non tanto secondo i convincimenti di chi manifesta il pensiero, quanto secondo le preferenze, i gusti e talora i capricci di chi ne è destinatario. Cosicché il pubblico apprende assai spesso non ciò che reputa giusto che sappia, ma ciò che pensa che gli piaccia di sapere».

Già allora infatti, contro il «rischio della manipolazione e della massificazione delle idee e delle anime», si auspicava «una nuova moderna battaglia del costituzionalismo, come tecnica della libertà» proponendo di «escogitare una sorta di *habeas mentem*, di *habeas animam*, e cioè un insieme di forme organizzative e procedurali a salvaguardia degli utenti, del loro diritto inviolabile, contro ogni tentativo di manipolazione e di spossessamento, a serbare intatta, almeno tra le mura della propria casa, la propria inconfondibile identità morale e culturale»²⁰. Il che presupponeva una distinzione tra condizionamento legittimo e illegittimo o, riprendendo le parole della giurisprudenza costituzionale a proposito del plagio, tra persuasione e suggestione.

16. SPINOZA 1670/1972, p. 480 ss.

17. PINELLI-RUFFOLO 2023, p. 9 ss.

18. CASSIRER 1971, p. 483.

19. PINELLI-RUFFOLO 2023, p. 10.

20. GALEOTTI 1979, p. 70.

Parole attuali, da poter riversare interamente a proposito di questi nuovi strumenti tecnologici, come ad esempio il *filter bubble*, uno stato di isolamento realizzato nell'ambito dei social network per mezzo di algoritmi in grado di effettuare ricerche personalizzate e sempre più in linea con gli interessi, le opinioni e le caratteristiche dell'utente. In tal modo, l'algoritmo, filtrando le notizie e le opinioni provenienti dal mondo esterno, restituisce all'utente solo ciò che è coerente con la visione della sua realtà, ponendo delicate questioni in termini di pluralismo dell'informazione.

Problema, dunque, con cui la dottrina già si era confrontata, senza tuttavia giungere a conclusioni tangibili. Eppure, il riconoscimento del principio di dignità, che le distingue da quelle del liberalismo ottocentesco, poteva sicuramente rappresentare il punto di partenza per individuare alcuni limiti alla capacità dell'artificio umano di manipolare i pensieri. Il peso della lunga tradizione che aveva considerato la libertà di pensiero come naturalmente incoercibile ha giocato certamente un ruolo importante²¹. Peraltro, anche le difficoltà inerenti alla esatta delimitazione, che abbia ovviamente un fondamento razionale-scientifico, dei confini tra autodeterminazione e eterodeterminazione – proprio perché l'essere umano non è solo mente, ma mente-corpo e, come tale, costantemente influenzato e direzionato dall'esterno – ha rappresentato un ostacolo rilevante.

Nella famosa sentenza n. 96 del 1981 sul plagio la Corte costituzionale, pur ritenendo la fattispecie penale indeterminata e, dunque, incostituzionale per violazione dell'art. 25 Cost., è partita, nella sua analisi, proprio dalla distinzione tra persuasione, che sarebbe lecita, e suggestione, che, al contrario, sarebbe illecita. La questione relativa alla violazione dell'art. 21 Cost. è stata ritenuta assorbita e, dunque, la Corte non si è espressa sulla eventuale tutela dell'integrità psichica e sulla libertà di autodeterminazione²².

Ci sono due possibili percorsi che è possibile intraprendere e che presuppongono due diverse declinazioni di una generica tutela della libertà di autodeterminazione.

Il primo è un percorso legato al concetto di democrazia. In estrema sintesi, il problema della libertà di autodeterminazione è prettamente politico e calato nel contesto di quello che una volta era il libero mercato delle idee. Presuppone il formarsi di una opinione pubblica scevra da condizionamenti esterni, intesi non solo con riferimento al territorio, per mano dunque di potenze straniere, ma anche come prodotto di campagne basate su una grande mole di notizie false, che ingenerano nel destinatario la percezione che siano vere; è il problema delle *fake news*, tramite l'utilizzo dell'intelligenza artificiale²³.

Il secondo è invece legato al riconoscimento di un vero e proprio diritto soggettivo di stampo costituzionale, presupposto di ogni altro diritto di libertà, che richiede l'individuazione di una norma costituzionale alla quale ancorarlo. Inoltre, in tal caso, assume maggiore rilevanza il problema della esatta individuazione di un fondamento razionale riscontrabile empiricamente.

Nel caso affrontato dalla Corte costituzionale sopra richiamato, la stessa ha affermato che «è estremamente difficile se non impossibile individuare sul piano pratico e distinguere a fini di conseguenze giuridiche – con riguardo ad ipotesi come quella in esame – l'attività psichica di persuasione da quella anche essa psichica di suggestione». Sul piano scientifico, non vi erano, ma probabilmente non ci sono ancora, «criteri sicuri per separare e qualificare l'una e l'altra attività e per accertare l'esatto confine fra esse. L'affermare che nella persuasione il soggetto passivo conserva la facoltà di scegliere in base alle argomentazioni rivoltegli ed è pertanto in grado di rifiutare e criticare, mentre nella suggestione la convinzione avviene in maniera diretta e irresistibile, profittando dell'altrui

21. PINELLI–RUFFOLO 2023, p. 10.

22. Sulla decisione v. AMARELLI 2015; BOSCARRELLI 1981; CACACE 2011; CHELI 2017; COLOMBO 2010; DALL'ONGARO 1982; GRASSO 1981.

23. V. EUROPEAN COMMISSION 2018. In dottrina cfr. SCIACCHITANO–PANZA 2020, p. 114 ss.; CLAUSSEN 2018, p. 136; PINELLI–RUFFOLO 2023; FROSINI 2017; MAZZIOTTI DI CELSO 2018; PINELLI–HASSAN 2022; PINELLI 2022; PITRUZZELLA–POLLICINO–QUINTARELLI 2017; LEHNER 2019, p. 119; PINELLI, 2017; CUNIBERTI 2017; BASSINI–VIGEVANI 2017; MELZI D'ERIL 2017; DE GREGORIO 2017; MONTI 2017; PIZZETTI 2017; ZANON 2018; PERRONE 2018.

impossibilità di critica e scelta, implica necessariamente una valutazione non solo dell'intensità dell'attività psichica del soggetto attivo, ma anche della qualità e dei risultati di essa»²⁴. In entrambi i casi, secondo la Corte, si tratterebbe di un accertamento del tutto incerto e affidato all'arbitrio del giudice.

Vassalli, non a caso, affermava che, mentre «la libertà personale è (...) una libertà esterna, la cui limitazione è facilmente riconoscibile ad occhio nudo», chi «potrebbe invece dirci – se non in casi-limite – quando sia stata effettivamente limitata o tolta la libertà morale?»²⁵.

In relazione al potere pubblico di coercizione di una libertà non fisica, ma appunto psichica, la Corte costituzionale ha avuto modo di riferirsi alla libertà morale e alla libertà di coscienza.

Con riferimento alla prima, nell'ambito di una giurisprudenza piuttosto altalenante, ha affermato, in una lontana decisione del 1962, la n. 30, che la garanzia prevista dall'art. 13 Cost. non deve essere intesa soltanto in rapporto alla coercizione fisica della persona, ma anche alla menomazione della libertà morale quando tale menomazione implichi un assoggettamento totale della persona all'altrui potere, capace di deformare artificialmente i naturali processi di autodeterminazione dell'individuo²⁶. Tesi ribadita e anche meglio precisata in tempi più recenti, ad esempio, nella decisione n. 419 del 1994, quando essa ha potuto chiarire che nella «degradazione giuridica» dell'individuo risiede l'elemento qualificante della restrizione della libertà personale e che per aversi tale «degradazione giuridica» è necessario che il provvedimento provochi una menomazione o una mortificazione della dignità o del prestigio della persona, tale da poter essere equiparata a quell'assoggettamento all'altrui potere in cui si concreta la violazione del principio dell'*habeas corpus*²⁷.

Con riferimento alla seconda, nella nota sentenza n. 467 del 1991, ha affermato che «a livello dei

valori costituzionali, la protezione della coscienza individuale si ricava dalla tutela delle libertà fondamentali e dei diritti inviolabili riconosciuti e garantiti all'uomo come singolo, ai sensi dell'art. 2 della Costituzione, dal momento che non può darsi una piena ed effettiva garanzia di questi ultimi senza che sia stabilita una correlativa protezione costituzionale di quella relazione intima e privilegiata dell'uomo con se stesso che di quelli costituisce la base spirituale-culturale e il fondamento di valore etico-giuridico. In altri termini, poiché la coscienza individuale ha rilievo costituzionale quale principio creativo che rende possibile la realtà delle libertà fondamentali dell'uomo e quale regno delle virtualità di espressione dei diritti inviolabili del singolo nella vita di relazione, essa gode di una protezione costituzionale commisurata alla necessità che quelle libertà e quei diritti non risultino irragionevolmente compressi nelle loro possibilità di manifestazione e di svolgimento a causa di preclusioni o di impedimenti ingiustificatamente posti alle potenzialità di determinazione della coscienza medesima»²⁸.

Sulla base di tale premessa, ne deriva che «quando sia ragionevolmente necessaria rispetto al fine della garanzia del nucleo essenziale di uno o più diritti inviolabili dell'uomo, quale, ad esempio, la libertà di manifestazione dei propri convincimenti morali o filosofici (art. 21 della Costituzione) o della propria fede religiosa (art. 19 della Costituzione) – la sfera intima della coscienza individuale deve esser considerata come il riflesso giuridico più profondo dell'idea universale della dignità della persona umana che circonda quei diritti, riflesso giuridico che, nelle sue determinazioni conformi a quell'idea essenziale, esige una tutela equivalente a quella accordata ai menzionati diritti, vale a dire una tutela proporzionata alla priorità assoluta e al carattere fondante ad essi riconosciuti nella scala dei valori espressa dalla Costituzione italiana. Sotto tale profilo, se pure a seguito di una delicata

24. Cfr. il punto 13 del Considerato in diritto.

25. VASSALLI 1997, p. 325 ss.

26. Cfr. il punto 2 del Considerato in diritto. In dottrina v. DE FRANCO 1962, p. 242 ss.; GALEOTTI 1962, p. 855 ss.; GUARNIERI 1962, p. 106 ss.; PIZZORUSSO 1962, p. 917 ss.

27. Cfr. il punto 3.2 del Considerato in diritto. V. i commenti di APRILE 1995; MOLINARI 1995.

28. Cfr. il punto 4 del Considerato in diritto. Cfr. ALIBRANDI 1992; DI COSIMO 1991; GALANTE 1996; GRAZIANO 1996; LUTHER 1992; MUSUMECI 1992; SASSI 1992.

opera del legislatore diretta a bilanciarla con contrastanti doveri o beni di rilievo costituzionale e a graduarne le possibilità di realizzazione in modo da non arrecar pregiudizio al buon funzionamento delle strutture organizzative e dei servizi d'interesse generale, la sfera di potenzialità giuridiche della coscienza individuale rappresenta, in relazione a precisi contenuti espressivi del suo nucleo essenziale, un valore costituzionale così elevato da giustificare la previsione di esenzioni privilegiate dall'assolvimento di doveri pubblici qualificati dalla Costituzione come inderogabili (c.d. obiezione di coscienza)²⁹.

Ricondurre tale diritto alla libertà psichica, concepito in una prospettiva slegata dalla dimensione biologico-corporea, come integrità fisica, la malattia nel corpo nella sua dimensione mentale, all'art. 2 o all'art. 13 non è ovviamente indifferente, posto che in quest'ultimo caso sarebbe necessario rispettare le garanzie della riserva di legge e della riserva di giurisdizione.

Nel suo lavoro "Filosofia e tecnologia" Finelli muove una forte critica all'ideologia dell'infosfera, che vorrebbe configurare l'intero mondo nella sua struttura elementare secondo processualità binarie-discrete, di natura informazionale, che, trascritte e codificate in linguaggio alfanumerico possono essere sottoposte a calcolo, a computazione, e comunicate a tutte le altre sorgenti programmate per decodificare e intendere quell'informazione³⁰.

A suo avviso, l'attività della mente umana «realizza operazioni autenticamente pensanti solo se esse muovono da sensazioni-emozioni di origine corporea e la psiche risulta dunque propriamente in attività solo quando riesce a trasformare le proprie emozioni in pensieri: in un transito che va costantemente dal corporeo emozionale al concettuale-rappresentativo e viceversa, secondo la *complementarietà disomogenea* delle facoltà che costituisce la struttura peculiare dell'essenza umana. *Il pensiero nasce dalla necessità di soddisfare le esigenze e le pulsioni del corpo (principio di piacere) nel confronto con la complessità della realtà esterna (principio di realtà)*. Nasce dalla necessità di contenere l'urgenza e l'invasività della dinamica

corporea nella dinamica psichica, attraverso un distanziamento/accoglimento della prima, che consenta di pensare e trovare la soluzione più adatta e più realistica (...) È, dunque, proprio nel benessere/malessere del corpo, nella riproduzione armonica e fisiologica, o asimmetrica e patologica, della sua omeostasi, che si origina la fonte prima e originaria del significato del nostro agire e pensare. Nel verso appunto del *valore di fondo* che indica, indirizza e giudica la direzione del nostro vivere»³¹.

Rimane ancora oggi arduo, anche se non impossibile, soprattutto con riferimento ai casi più estremi, ancorarlo a parametri scientifici falsificabili, proprio in virtù della connessione inscindibile mente-corpo. Il venir meno del dualismo cartesiano ha reso, in un certo senso, più complesso individuare un'area autonoma della mente e, conseguentemente, un parametro oggettivamente determinabile a cui ancorare la relativa protezione.

Ciononostante, il regolamento sull'IA contiene un art. 5 molto netto, almeno sulla carta: tale norma individua le pratiche di intelligenza artificiale vietate, facendo riferimento, in prima battuta, ai sistemi di IA che utilizzano tecniche subliminali, manipolative o ingannevoli, con l'obiettivo di distorcere materialmente il comportamento di una persona o di un gruppo di persone, pregiudicandone sensibilmente la capacità di prendere una decisione informata e inducendola, in tal modo, a prendere una decisione che non avrebbe altrimenti preso o producendole, probabilmente, un danno significativo. Un precedente, per certi versi simile, è rinvenibile, in ambito nazionale, nell'art. 188 c.p.p., rubricato infatti "Libertà morale della persona nell'assunzione della prova", ai sensi del quale «non possono essere utilizzati, neppure con il consenso della persona interessata, metodi o tecniche idonei a influire sulla libertà di autodeterminazione o ad alterare la capacità di ricordare e di valutare i fatti». La norma pone infatti un principio, considerato di ordine generale, per cui l'ordinamento rifiuta l'assunzione delle prove nell'ambito del processo penale mediante l'utilizzo di modalità che possano manipolare la libertà morale della persona. La *ratio* del rifiuto è dunque individuata nella necessità di garantire tanto la dignità della

29. Cfr. ancora il punto 4 del Considerato in diritto.

30. FINELLI 2022, p. 18.

31. *Ivi*, p. 21, corsivi dell'Autore.

persona, quanto l'attendibilità della prova, ritenuta più genuina e vicina alla verità storica quando realizzata attraverso il rispetto della sua libertà di autodeterminazione.

Il profilo della dignità della persona viene in rilievo in tutte le pratiche vietate dall'art. 5. Si prevede infatti, in secondo luogo, il divieto anche di quei sistemi di IA che sfruttano le vulnerabilità di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona che appartiene a tale gruppo in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico; di quelli che vengono utilizzati dalle autorità pubbliche o per loro conto ai fini della valutazione o della classificazione dell'affidabilità delle persone fisiche per un determinato periodo.

Norme dal contenuto innovativo, da valutare alla prova dell'effettività.

Con riferimento al primo percorso, venuto meno l'entusiasmo per la Rete quale arena di un pieno sviluppo del "libero mercato delle idee" e la convinzione che l'autoregolamentazione dei titolari delle piattaforme fosse sufficiente per contrastare la disinformazione, dopo alcune leggi approvate in alcuni Stati membri dell'Unione europea, è stato varato un regolamento dell'Unione specifico sul tema, il *Digital Service Act* (DSA). Anche qui il tempo ci dirà se trattasi di effetto Bruxelles o altro³².

Inoltre, con l'art. 3 del disegno di legge sull'intelligenza artificiale presentato dal Governo, rubricato "Principi generali", il legislatore nazionale ha stabilito, al comma 3, che i sistemi e i modelli di intelligenza artificiale devono essere sviluppati e applicati nel rispetto della autonomia e del potere decisionale dell'uomo, della prevenzione del danno, della conoscibilità, della spiegabilità e dei principi di cui al comma 1, ossia nel rispetto dei diritti fondamentali e delle libertà previste dalla Costituzione, del diritto dell'Unione europea e dei principi di trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità, mentre, al comma 4, che l'utilizzo

di sistemi di intelligenza artificiale non deve pregiudicare lo svolgimento con metodo democratico della vita istituzionale e politica.

In ogni caso, la Corte costituzionale, nella famosissima sentenza n. 16 del 1978 a proposito del referendum abrogativo, aveva ritenuto che l'art. 75 non implicasse affatto «l'ammissibilità di richieste comunque strutturate, comprese quelle eccedenti i limiti esterni ed estremi delle previsioni costituzionali, che conservino soltanto il nome e non la sostanza del referendum abrogativo. Se è vero che il referendum non è fine a se stesso, ma tramite della sovranità popolare, occorre che i quesiti posti agli elettori siano tali da esaltare e non da coartare le loro possibilità di scelta; mentre è manifesto che un voto bloccato su molteplici complessi di questioni, insuscettibili di essere ridotte ad unità, contraddice il principio democratico, incidendo di fatto sulla libertà del voto stesso (in violazione degli artt. 1 e 48 Cost.). (...) Uno strumento essenziale di democrazia diretta, quale il referendum abrogativo, non può essere infatti trasformato – insindacabilmente – in un distorto strumento di democrazia rappresentativa, mediante il quale si vengano in sostanza a proporre plebisciti o voti popolari di fiducia, nei confronti di complessive inscindibili scelte politiche dei partiti o dei gruppi organizzati che abbiano assunto e sostenuto le iniziative referendarie»³³.

La sentenza in commento assume particolare rilevanza anche in vista della classica obiezione per cui ciò che vale per il potere pubblico non può – e non deve – valere anche per il potere privato.

La società analogica era fondata sul principio di rappresentanza, sulla presenza di corpi intermedi, sulla trasparenza dei metodi di formazione delle classi politiche dirigenti, sul controllo del loro operato e sulla loro sostituibilità. L'intermediazione era uno strumento utile per filtrare le informazioni e per stimolare il dibattito in vista di un agire consapevole e autonomo, ma, come è stato detto, non è in corso una disintermediazione, bensì una sostituzione occulta dei mediatori³⁴, l'affermazione del principio per cui la sovranità appartiene ai poteri (pubblici e privati) digitali, che la esercitano nelle forme e nei limiti dell'intelligenza artificiale.

32. Il c.d. "effetto Bruxelles", su cui v. BRADFORD 2020.

33. Cfr. il punto 5 del Considerato in diritto.

34. VIOLANTE 2019.

Dobbiamo dunque capire quali siano le differenze connotative tra intelligenza artificiale e essere umano e fare in modo di proteggere queste differenze.

Fioravanti, in un saggio su passato, presente e futuro dello Stato costituzionale ha sostenuto: «per quanto riguarda il futuro non si può fare a meno di ricordare il secondo comma dell'articolo terzo della medesima Costituzione italiana, dove l'incidere fin dall'inizio nel senso che è “Compito della Repubblica” operare nella società per promuovere lo sviluppo della personalità di ognuno, e insieme una cittadinanza attiva e consapevole, perché munita dei beni essenziali dell'istruzione, della assistenza in caso d'invalidità, e del lavoro. La verità è che lo Stato di diritto dell'Ottocento sembrava essere assai più solido e sicuro dello Stato costituzionale che verrà, e che si va formando nel nostro

presente. Quella dello Stato di diritto era per altro una sicurezza tutta calata nel presente, tendenzialmente priva di passato, cui si ricorreva per la sola fondazione dei diritti, e di futuro, visto solo come mero perfezionamento del presente medesimo. Lo Stato costituzionale di oggi è ben diverso. Esso ha un'esistenza immediata ben più difficile e precaria, perché data sulla base delle norme di principio. Ma proprio per lo stesso motivo è anche infinitamente più ambizioso, perché aperto al passato e proiettato verso il futuro»³⁵.

Il giurista, il costituzionalista, non può limitarsi all'osservazione; al contrario, una volta osservato, deve riflettere, distinguere, categorizzare, suggerire dunque ipotesi di intervento, proporre, lui sì, ipotesi di condizionamento, affinché l'agire umano sia, per quanto possibile, conforme ai principi costituzionali e, dunque, al proprio sentire.

Riferimenti bibliografici

- AA.VV. (2024), *Il futuro del diritto pubblico. Il tempo e le sfide*, in “Diritto pubblico”, 2024, n. 1
- G. AMARELLI (2015), *Il principio di determinatezza e il delitto di atti persecutori alla luce della sentenza della Corte costituzionale n. 172/2014*, in “Studium iuris”, 2015, n. 7-8
- E. APRILE (1995), *La Corte costituzionale “corregge” la disciplina della misura del soggiorno cautelare anti-mafia (nota)*, in “Il Nuovo Diritto”, 1995, n. 4
- A. ALIBRANDI (1992), *In tema di tardiva obiezione di coscienza al servizio militare*, in “Rivista penale”, 1992, n. 4
- M. BASSINI, G.E. VIGEVANI (2017), *Primi appunti su fake news e dintorni*, in “MediaLaws. Rivista di Diritto dei Media”, 2017, n. 1
- R. BODEI (2019), *Dominio e sottomissione. Schiavi, animali, macchine, Intelligenza Artificiale*, il Mulino, 2019
- M. BOSCARELLI (1981), *A proposito del “principio di tassatività”*, in “Rivista italiana di diritto e procedura penale”, 1981, n. 3
- A. BRADFORD (2020), *The Brussel Effect. How the European Union Rules the World*, Oxford University Press, 2020
- E. CACACE (2011), *Riserva di legge e fattispecie penale: relazioni tra fonti primarie e secondarie*, in “Giurisprudenza costituzionale”, 2011, n. 6
- A. CARLEO (a cura di) (2017), *Calcolabilità giuridica*, il Mulino, 2017
- E. CASSIRER (1971), *Il mito dello Stato*, Longanesi, 1971
- E. CHELI (2017), *Scienza, tecnica e diritto: dal modello costituzionale agli indirizzi della giurisprudenza costituzionale*, in “Rivista AIC”, 2017, n. 1

35. FIORAVANTI 2018, p. 9.

- V. CLAUSSEN (2018), *Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation*, in “MediaLaws. Rivista di Diritto dei Media”, 2018, n. 3
- C. COLOMBO (2010), *La manipolazione mentale e le sette sataniche tra fattispecie penali e diritti costituzionalmente garantiti*, in “Rivista penale”, 2010, n. 11
- M. CUNIBERTI (2017), *Il contrasto alla disinformazione in rete tra logiche del mercato e (vecchie e nuove) velleità di controllo*, in “MediaLaws. Rivista di Diritto dei Media”, 2017, n. 1
- F. DALL’ONGARO (1982), *L’illegittimità costituzionale del reato di plagio*, in “Il diritto di famiglia e delle persone”, 1982, n. 2
- R.G. DE FRANCO (1962), *Ancora in tema di rilievi segnaletici di P.S.*, in “Giurisprudenza costituzionale”, 1962, n. 1
- G. DE GREGORIO (2017), *The market place of ideas nell’era della post-verità: quali responsabilità per gli attori pubblici e privati online?*, in “MediaLaws. Rivista di Diritto dei Media”, 2017, n. 1
- G. DI COSIMO (1991), *Coscienza individuale e momento di manifestazione dell’obiezione al servizio militare*, in “Giurisprudenza costituzionale”, 1991, n. 6
- EUROPEAN COMMISSION (2018), *A multi-dimensional approach to disinformation. Final report of the High Level Expert Group on Fake News and Online Disinformation*, 12 March 2018
- R. FINELLI (2022), *Filosofia e tecnologia. Una via di uscita dalla mente digitale*, Rosenberg & Sellier, 2022
- M. FIORAVANTI (2018), *Passato, presente e futuro dello Stato costituzionale odierno*, in “Nomos. Le attualità del diritto”, 2018, n. 2
- T.E. FROSINI (2017), *No news is fake news*, in “Diritto pubblico comparato ed europeo”, 2017, n. 4
- G. GALANTE (1996), *Spunti critici nella giurisprudenza costituzionale più o meno recente in materia di obiezione di coscienza al servizio militare*, in “Giurisprudenza costituzionale”, 1996, n. 2
- G. GALEOTTI (1979), *Le strutture dell’informazione in Italia*, in Unione giuristi cattolici italiani, “Problemi giuridici dell’informazione” (Atti del XXVIII Convegno nazionale di studio, Roma, 9-11 dicembre 1977), Giuffrè, 1979
- S. GALEOTTI (1962), *Rilievi segnaletici e restrizione della libertà personale*, in “Rivista italiana di diritto e procedura penale”, 1962
- P.G. GRASSO (1981), *Controllo sulla rispondenza alla realtà empirica delle previsioni legali di reato*, in “Giurisprudenza costituzionale”, 1981, n. 6
- L. GRAZIANO (1996), *Riflessi nel tempo dell’azione della Corte Costituzionale sulla normativa del fenomeno religioso*, in “Il diritto ecclesiastico”, 1996, n. 1
- G. GUARNIERI (1962), *Limiti costituzionali all’ammissibilità dell’ispezione personale ad opera della polizia*, in “La Scuola positiva”, 1962
- N. IRTI (2017), *Per un dialogo sulla calcolabilità giuridica*, in A. Carleo (a cura di), “Calcolabilità giuridica”, il Mulino, 2017
- E. LEHNER (2019), *Fake news e democrazia*, in “MediaLaws. Rivista di Diritto dei Media”, 2019, n. 1
- A. LONGO (2016), *Tempo interpretazione Costituzione. Premesse teoriche*, I, Editoriale Scientifica, 2016
- M. LUCIANI (2018), *La decisione giudiziaria robotica*, in “Rivista AIC”, 2018, n. 3
- J. LUTHER (1992), *I diritti della coscienza in attesa di una nuova legge*, in “Giurisprudenza italiana”, 1992, n. 4

- G. MARRAMAO (2021), *Quale futuro per il Post-umano? L'umano*, in Aa.Vv., [“Privacy e neurodiritti. La persona al tempo delle neuroscienze”](#), Atti del Convegno organizzato dal Garante per la protezione dei dati personali in occasione della “Giornata europea della protezione dei dati personali”, 2021
- D. MARTIRE (2022), *Intelligenza artificiale e Stato costituzionale*, in “Diritto pubblico”, 2022, n. 2
- A. MAZZIOTTI DI CELSO (2018), *Dal Primo Emendamento al bavaglio malese. Fake news, libertà di espressione e il rovesciamento delle categorie politiche tradizionali*, in “MediaLaws. Rivista di Diritto dei Media”, 2018, n. 3
- C. MELZI D'ERIL (2017), *Fake news e responsabilità: paradigmi classici e tendenze incriminatrici*, in “MediaLaws. Rivista di Diritto dei Media”, 2017, n. 1
- P.V. MOLINARI (1995), *Alcune riflessioni sul soggiorno cautelare riscritto in gran parte dalla Corte costituzionale*, in “Cassazione penale”, 1995, n. 3
- M. MONTI (2017), *Fake news e social network: la verità ai tempi di Facebook*, in “MediaLaws. Rivista di Diritto dei Media”, 2017, n. 1
- A. MUSUMECI (1992), *Obiezione di coscienza e giudizio di legittimità nell'ottica dei valori*, in “Giurisprudenza costituzionale”, 1992, n. 1
- R. PERRONE (2018), *Fake news e libertà di manifestazione del pensiero: brevi coordinate in tema di tutela costituzionale del falso*, in “Nomos. Le attualità del diritto”, 2018, n. 2
- C. PINELLI (2022), *Disinformazione, comunità virtuali e democrazia: un inquadramento costituzionale*, in “Diritto pubblico”, 2022, n. 1
- C. PINELLI (2017), *“Postverità”, verità e libertà di manifestazione del pensiero*, in “MediaLaws. Rivista di Diritto dei Media”, 2017, n. 1
- C. PINELLI, C. HASSAN (2022), *Disinformazione e democrazia. Populismo, rete e regolazione*, Marsilio, 2022
- C. PINELLI, U. RUFFOLO (2023), *I diritti nelle piattaforme*, Giappichelli, 2023
- G. PITRUZZELLA, O. POLLICINO, S. QUINTARELLI (2017), *Parole e potere. Libertà d'espressione, hate speech e fake news*, Egea, 2017
- F. PIZZETTI (2017), *Fake news e allarme sociale: responsabilità, non censura*, in “MediaLaws. Rivista di Diritto dei Media”, 2017, n. 1
- A. PIZZORUSSO (1962), *Nota s.t.*, in “Giurisprudenza italiana”, 1962, n. 1
- P. SASSI (1992), *Una nuova sentenza della Corte costituzionale in tema di obiezione di coscienza al servizio militare. Obiezione c.d. sopravvenuta e motivi religiosi*, in “Giurisprudenza costituzionale”, 1992, n. 1
- F. SCIACCHITANO, A. PANZA (2020), *Fake news e disinformazione online: misure internazionali*, in “MediaLaws. Rivista di Diritto dei Media”, 2020, n. 1
- A. SIMONCINI (2019), *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in “BioLaw Journal”, 2019, n. 1
- B. SPINOZA (1670/1972), *Trattato teologico-politico*, Einaudi, 1972
- P. STANZIONE (2021), *Relazione introduttiva*, in Aa.Vv., [“Privacy e neurodiritti. La persona al tempo delle neuroscienze”](#), Atti del Convegno organizzato dal Garante per la protezione dei dati personali in occasione della “Giornata europea della protezione dei dati personali”, 2021
- G. VASSALLI (1997), *Il diritto alla libertà morale (Contributo alla teoria dei diritti della personalità)*, in Studi in memoria di Filippo Vassalli, II, Utet, 1960, ora in G. Vassalli, “Scritti giuridici, III, Il processo e le libertà”, Giuffrè, 1997

- L. VIOLANTE (2019), *Rifondare la democrazia nella società digitale*, in “Corriere della Sera”, 26 ottobre 2019
- G. ZAGREBELSKY, V. MARCENÒ (2018), *Giustizia costituzionale. Storia, principi, interpretazioni*, I, il Mulino, 2018
- N. ZANON (2018), *Fake news e diffusione dei social media: abbiamo bisogno di una “Autorità pubblica della verità”?*, in “MediaLaws. Rivista di Diritto dei Media”, 2018, n. 1



RIVISTA ITALIANA DI
INFORMATICA E DIRITTO

PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0162 • articolo sottoposto a peer review • pubblicato in anteprima il 4 ott. 2024
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale 

CRISTINA NAPOLI

Strumenti informatici nel processo decisionale amministrativo ed effettività del diritto di difesa: questioni vecchie e problemi nuovi alla luce del Regolamento (UE) 2024/1689

Il saggio, anche alla luce della recentissima adozione del Regolamento (UE) 2024/1689 (Regolamento sull'intelligenza artificiale), propone una riflessione sulla devoluzione della formazione della volontà pubblica a un sistema programmato e istruito di elaborazione di dati e dunque sulle ricadute che tale opzione determina con riguardo all'esercizio del diritto di difesa da parte del destinatario del provvedimento finale.

Algoritmi – Intelligenza artificiale – Decisione amministrativa – Diritto di difesa

Information technology tools in administrative decision making and effectiveness of the right to defense: old issues and new problems taking into consideration Regulation (EU) 2024/1689

The essay, also taking into consideration the very recent adoption of Regulation (EU) 2024/1689 (Artificial Intelligence Act), proposes a reflection on the devolution of the formation of public will to a programmed and instructed system of data processing and therefore on the repercussions that this choice determines on the exercise of the right to defense by the subject to whom the final measure is addressed.

Algorithms – Artificial intelligence – Administrative decision – Right of defense

L'Autrice è ricercatrice di Istituzioni di diritto pubblico presso Sapienza – Università di Roma

Questo contributo fa parte della sezione monografica *Cittadini e pubbliche amministrazioni tra AI e diritto all'umano*, a cura di Enrico Carloni

SOMMARIO: 1. La proiezione verso l'esterno dell'amministrazione digitale. Delimitazione dell'oggetto dell'indagine. – 2. Qualche notazione preliminare sulla diffusione di algoritmi e sistemi c.d. intelligenti in luogo dell'attività umana. – 3. L'automazione del processo decisionale da parte dell'autorità pubblica nel Regolamento (UE) 2016/679. – 4. Il ricorso a decisioni automatizzate da parte della pubblica amministrazione nell'ordinamento italiano. – 4.1. *Dal funzionario dominus del procedimento alla soddisfazione attraverso l'algoritmo del principio di buon andamento.* – 4.2. *Le categorie tradizionali del diritto pubblico quale ineludibile lente di osservazione.* – 5. La posizione del destinatario finale del provvedimento e il diritto effettivo di difesa in giudizio nella giurisprudenza amministrativa. – 5.1. *L'accessibilità e la comprensibilità della formula tecnica che si traduce in regola giuridica.* – 5.2. *L'imputabilità della decisione e della relativa responsabilità all'organo titolare del potere.* – 5.3. *Il carattere non discriminatorio dell'algoritmo.* – 5.4. *La sindacabilità da parte del giudice amministrativo.* – 6. Gli sviluppi più recenti in tema di intelligenza artificiale antropocentrica e affidabile nel Regolamento (UE) 2024/1689. – 7. Lo spazio di intervento del legislatore nazionale e la necessaria alfabetizzazione in tema di intelligenza artificiale. Considerazioni conclusive.

1. La proiezione verso l'esterno dell'amministrazione digitale. Delimitazione dell'oggetto dell'indagine

Nel “Rapporto sui principali problemi dell'Amministrazione dello Stato” a cura del Ministero della Funzione Pubblica del 1979 un'intera sezione veniva dedicata alla *Tecnologia delle amministrazioni* e all'interno di questa, nel paragrafo intitolato *L'attività di informatica*, veniva rilevato come i sistemi informativi nella disponibilità delle amministrazioni, peraltro ritenuti inadeguati alle esigenze qualitative e quantitative dell'attività amministrativa, lungi dal servire per soli «fatti di gestione interna»,

mostrassero col passare del tempo l'attitudine al vero e proprio amministrare, proiettandosi, cioè, «sempre più verso l'esterno»¹.

Ciò nonostante, il processo d'informatizzazione della pubblica amministrazione, anche a seguito dell'invito rivolto dalla Commissione europea agli Stati membri a contribuire alla formazione di una società della conoscenza attraverso il rafforzamento del c.d. *e-government*², può dirsi concretamente avviato nell'ordinamento italiano soltanto a seguito dell'entrata in vigore del d.lgs. n. 82/2005, con cui le tecnologie dell'informazione e della comunicazione (ICT) vengono a essere considerate strumenti grazie ai quali le pubbliche amministrazioni

1. Il *Rapporto*, trasmesso alle Camere il 16 novembre 1979 dall'allora Ministro per la funzione pubblica Massimo Severo Giannini, è reperibile in “Foro Italiano”, 1979, V, vol.102, c. 289 ss.

2. Cfr. Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni su *Il ruolo dell'eGovernment per il futuro dell'Europa* – [COM\(2003\) 567](#) – ove l'*e-government* è definito come «l'uso delle tecnologie dell'informazione e della comunicazione nelle Pubbliche Amministrazioni, coniugato a modifiche organizzative e all'acquisizione di nuove competenze al fine di migliorare i servizi pubblici e i processi democratici e di rafforzare il sostegno alle politiche pubbliche».

possono organizzare la propria attività «per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione»³. Il Codice dell'amministrazione digitale è in costante evoluzione e aggiornamento e in tempi relativamente recenti è stato oggetto di profonde modificazioni e integrazioni a opera dei decreti legislativi emanati ai sensi dell'art. 1 legge n. 124/2015 in materia di riorganizzazione delle amministrazioni pubbliche⁴.

Il tema su cui si intende in questa sede proporre una riflessione, tuttavia, non attiene alle modalità con cui la pubblica amministrazione esterna la propria volontà⁵ e neppure a quelle con cui essa comunica con altri soggetti pubblici o privati⁶, bensì all'ipotesi che la formazione della volontà pubblica sia devoluta a un sistema programmato e istruito di elaborazione di dati e dunque alle ricadute che tale opzione determina con riguardo all'esercizio del diritto di difesa da parte del destinatario del provvedimento finale.

A questo proposito, può essere il caso di rilevare già in apertura come la domanda di ricerca tragga linfa dalla necessità di verificare se e in quale misura l'adozione da ultimo del Regolamento (UE) 2024/1689 (Regolamento sull'intelligenza artificiale) si ripercuota sull'oggetto dell'indagine, con riferimento al quale, invero, muovendo dai principi e dai contenuti di cui al Regolamento (UE) 2016/679 (Regolamento generale sulla protezione dei dati), si è assistito in tempi pure recenti al consolidamento di precisi orientamenti giurisprudenziali.

2. Qualche notazione preliminare sulla diffusione di algoritmi e sistemi c.d. intelligenti in luogo dell'attività umana

È fatto del tutto notorio come il ricorso ad algoritmi informatici per risolvere problemi e/o assumere decisioni interessi ormai ogni campo dell'agire umano. A tali procedure di calcolo che «sin dalla nozione desunta dai papiri di Ahmes del XVII secolo a.c. [...] consent[ono], attraverso un insieme di operazioni effettuate in un determinato ordine, partendo da un insieme di dati (input), di ottenere un risultato atteso (output)»⁷, sono invero riconosciuti vantaggi di non secondaria importanza, quantomeno sotto i profili dell'efficienza e della neutralità: da un lato, infatti, la trasformazione di un input in un output da parte di una macchina dovrebbe essere in grado di eliminare quella percentuale di errore umano che in particolare nell'esecuzione di operazioni ripetitive pare non arginabile⁸; dall'altro lato, nondimeno, l'utilizzo di asettiche operazioni matematiche effettuate attraverso l'algoritmo e lo strumento elettronico a servizio di esso dovrebbe pure servire a eludere quelle falle tipiche dei processi cognitivi umani che conducono a esiti non sempre ragionevoli e imparziali⁹.

La nascita e lo sviluppo della c.d. intelligenza artificiale quale branca dell'informatica, poi, ha reso il fenomeno ancora più irreversibile grazie alla creazione, attraverso essa, di sistemi capaci di garantire alle macchine prestazioni considerate tipiche dei meccanismi intellettivi dell'essere umano¹⁰: in questo senso, con l'affermazione

3. Cfr. art. 12, co. 1, d.lgs. 7 marzo 2005, n. 82.

4. Cfr. d.lgs. 26 agosto 2016, n. 179 e d.lgs. 13 dicembre 2017, n. 217.

5. Sull'atto amministrativo c.d. informatico pionieristicamente v. MASUCCI 1993. Cfr. art. 40 d.lgs. 82/2005.

6. Cfr. art. 12, co. 2, d.lgs. n. 82/2005.

7. Così Consiglio di Stato, sez. VI, sentenza n. 2270/2019.

8. Per quanto esistano problemi per i quali non è nota una soluzione efficiente (c.d. problemi NP-completi), una delle principali proprietà dell'algoritmo è proprio l'efficienza da intendersi come «la velocità ovvero quanto tempo impiega un algoritmo per produrre il suo risultato», cfr. CORMEN-LEISERSON-RIVEST-STEIN 2010, p. 8.

9. Sugli studi in materia di psicologia cognitiva ed economia comportamentale ci si limita a rinviare a REVLIN 2014 e ANGNER 2017.

10. Dalla *cibernetica* quale scienza del controllo e della comunicazione nella macchina e negli esseri viventi (secondo la definizione di WIENER 1948) all'elaborazione del noto *test di Turing* avente l'obiettivo di determinare la capacità o meno di una macchina di pensare (cfr. TURING 1950, pp. 433-460), il concetto di intelligenza artificiale si afferma sul finire degli anni Cinquanta del secolo scorso grazie all'intuizione di un gruppo di studiosi, riunitisi nell'estate del 1956 in occasione di un convegno presso il Dartmouth college di Hanover, circa la possibilità

e la diffusione di tale disciplina, l'uso di sistemi intelligenti ha finito per ricevere una tale quantità di applicazioni concrete e, soprattutto, di quotidiana utilità, da rendere non sempre e non del tutto immediata la percezione della mole di attività tradizionalmente umana ormai svolta dalle macchine¹¹.

Può essere opportuno sottolineare come la nozione di algoritmo, ove applicata a sistemi tecnologici, sia strettamente connessa «al concetto di automazione, ossia a sistemi di azione e controllo idonei a ridurre l'intervento umano» l'entità del quale dipende «dalla complessità e dall'accuratezza dell'algoritmo che la macchina è chiamata a processare». Ciò differisce dalla nozione di intelligenza artificiale con riferimento alla quale invece «l'algoritmo contempla meccanismi di *machine learning* e crea un sistema che non si limita solo ad applicare le regole software e i parametri preimpostati [...] ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico»¹².

La scansione procedimentale tipica del funzionamento dei meccanismi in argomento, distinta in

tre fasi, comprende (i) l'immissione, come input della procedura di calcolo, di dati, ormai disponibili in quantità sempre più massicce¹³; (ii) l'elaborazione di tali dati attraverso apposito trattamento; (iii) la produzione a valle della procedura di un output apprezzabile in termini decisori, tenendo presente che l'utilizzo in via esclusiva di strumenti tecnologici qualifica la procedura decisionale e per tale via la decisione stessa come automatizzata.

3. L'automazione del processo decisionale da parte dell'autorità pubblica nel Regolamento (UE) 2016/679

Dall'emersione in via giurisprudenziale delle iniziali forme di tutela dei dati¹⁴, le dimensioni che il fenomeno descritto nel paragrafo precedente ha nel tempo assunto ben si colgono volgendo lo sguardo all'attenzione che il diritto eurounitario ha gradualmente riposto sull'affermazione e sul consolidamento di una disciplina specificamente dedicata ai dati e al relativo utilizzo¹⁵.

In questo senso, alla prima sistematizzazione della materia realizzata a opera della direttiva 95/46/CE¹⁶ ha fatto seguito l'entrata in vigore del regolamento del Parlamento europeo e del Consiglio 2016/679 il

di descrivere ogni aspetto dell'intelligenza umana con un livello tale di precisione da consentirne a una macchina la ripetizione. Senza pretese di esaustività, in disparte gli studi sulle applicazioni della disciplina nelle diverse branche del sapere, v. FINK 1967; AIRENTI-BARA 1978; SOMALVICO 1987; TABOSS 1988; CARLUCCI AIELLO-CIALDEA MAYER 1995; BOZZO 1996; VAIANA 1996; NEGNEVITSKY 2002; NILSSON 2002; RUSSELL-NORVIG 2021; SEVERINO 2022; KISSINGER-SCHMIDT-HUTTENLOCHER 2023.

11. Tra i primi studi italiani sull'impatto dello sviluppo delle scienze informatiche sul diritto e sulla società v. FROSINI 1968; RODOTÀ 1973.
12. Così Consiglio di Stato, sez. III, n. 7891/2021.
13. Sul tema dei big data nella letteratura più recente v., almeno, REZZANI 2013; MAYER-SCHÖNBERGER-CUKIER 2013; MONINO-SEDKAOUI 2016; PEDRYCZ-CHEN 2017; DELLA MORTE 2018; DELMASTRO-NICITA 2019; PEDERSEN 2019. Sui metodi analitici, ci si limita a segnalare DE LUCA 2018; GHAVAMI 2019; PRABHU-SREEVALLABH CHIVUKULA-MOGADALA et al. 2019; CAVALLO PERIN 2021; NUMERICO 2021.
14. Sull'iniziale emersione di un diritto alla protezione dei dati personali dapprima nelle «pieghe del sistema di protezione della Cedu da parte della Corte di Strasburgo» e, dunque, nella giurisprudenza della Corte di Lussemburgo v. TIBERI 2007, p. 373 ss. Cfr. anche DE HERT-GUTWIRTH 2009, p. 18 ss.; MIDIRI 2016, part. 2 e 3. In ambito convenzionale, la necessità di armonizzare le normative prodotte in vari Stati europei e caratterizzate da più che differenziati livelli di tutela, nonché di neutralizzare l'effetto derivante dall'inesistenza in taluni altri di qualsivoglia regolamentazione in materia condusse il Consiglio d'Europa all'approvazione della *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale*, sottoscritta a Strasburgo il 28 gennaio 1981 e ratificata in Italia con l. 21 febbraio 1989, n. 98.
15. Sulle ricadute della rivoluzione digitale in tema di privacy v. BUSIA-LIGUORI-POLLICINO 2016.
16. Direttiva del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. A essa hanno fatto seguito

quale, ai sensi dell'art. 8 Carta dei diritti fondamentali dell'Unione europea¹⁷, detta norme sulla protezione delle persone fisiche circa il trattamento dei dati personali e sulla libera circolazione di essi¹⁸.

Non essendo questa la sede per soffermarsi diffusamente sui contenuti del GDPR¹⁹, con particolare riferimento al tema che viene qui in considerazione è certo che anche l'autorità pubblica, oltre ai soggetti privati, possa senz'altro *trattare i dati* a sua disposizione²⁰, cosicché sicuro interesse riveste la possibilità che l'intero procedimento decisionale pubblico possa svolgersi in via esclusivamente automatizzata²¹.

A tale proposito, può dirsi che, in esecuzione dell'art. 15 (*Decisioni individuali automatizzate*) della direttiva 95/46/CE, l'art. 14 d.lgs. n. 196/2003 aveva originariamente escluso che un «atto o provvedimento giudiziario o amministrativo» implicante «una valutazione del comportamento umano» potesse «essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato».

Con l'entrata in vigore del regolamento 2016/679, il processo decisionale automatizzato

ha trovato la propria sede normativa direttamente all'interno del GDPR e in specie dell'art. 22 il quale, in maniera non dissimile dalla previgente disciplina europea²², ha previsto la possibilità di derogare al principio di non esclusività della decisione algoritmica in presenza di talune circostanze²³.

L'art. 22, infatti, nonostante affermi in apertura l'esistenza in capo al soggetto interessato di un diritto «di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione», cosicché l'intervento umano, effettivo, non simbolico e funzionale al riesame degli esiti del processo automatizzato, dovrebbe sempre avere luogo²⁴, ha circoscritto l'applicabilità di tale limite a quelle decisioni che producono «effetti giuridici» ovvero che incidono «in modo analogo significativamente sulla sua persona»²⁵.

Potenzialmente amplissime eccezioni alla regola generale risultano ancora menzionate nel paragrafo 2 del medesimo art. 22 secondo cui questa non trova applicazione ove la decisione (a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, (b)

le direttive 97/66/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni e 2002/58/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle comunicazioni elettroniche. L'attuazione nell'ordinamento italiano è riconducibile dapprima alla legge n. 675/1996 e in un secondo momento al d.lgs. n. 196/2003.

17. Cfr. POLLICINO-BASSINI 2017, p. 134 ss.

18. Il regolamento n. 679/2016 ha abrogato la direttiva 95/46/CE. A seguito dell'emanazione del GDPR, con il d.lgs. 10 agosto 2018, n. 101 la normativa nazionale in materia e in specie quella contenuta nel d.lgs. 30 giugno 2003, n. 196 è stata a esso adeguata. Cfr. PIZZETTI 2018.

19. Per un approfondimento sul tema dei dati, delle categorie di dati, del relativo trattamento e della decisione automatizzata nel GDPR si rinvia a NAPOLI 2020, pp. 322-329.

20. Cfr. art. 4, par. 1, nn. 7 e 8 GDPR per la nozione di «titolare» e di «responsabile del trattamento».

21. A tale proposito si segnala come il 3 ottobre 2017 venivano adottate le *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679* dal Gruppo di lavoro istituito ai sensi dell'art. 29 direttiva 95/46/CE.

22. I contenuti del richiamato art. 15 della direttiva 95/46/CE sono infatti confluiti, per quanto rielaborati, nell'art. 22 del regolamento 2016/679.

23. L'art. 14 è stato abrogato dall'art. 27, co. 1, lett. a), n. 2), d.lgs. n. 101/2018.

24. Art. 22, par. 1 GDPR. V. anche considerando n. 71.

25. Le *Linee guida sul processo decisionale automatizzato* elaborate dal Gruppo di lavoro articolo 29 hanno sin da subito ricondotto (i) le prime a quelle decisioni che incidono «sui diritti giuridici di una persona, quali la libertà di associarsi ad altre persone, di votare nel contesto di un'elezione o di intraprendere azioni legali» ovvero «sullo status giuridico di una persona o sui suoi diritti ai sensi di un contratto» e (ii) le seconde a quelle che influiscono in maniera significativa sulle circostanze, sul comportamento o sulle scelte dell'interessato, che hanno un impatto prolungato o permanente sull'interessato o che comportano effetti discriminatori sulle persone.

sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, (c) si basi sul consenso esplicito dell'interessato.

Ai sensi del successivo paragrafo 3, poi, nelle ipotesi di cui *sub a)* e *c)*, «il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione».

Si sottolinea, peraltro, che le deroghe appena richiamate si estendono anche alle decisioni relative ai dati c.d. *sensibili*, per quanto l'estensione sia circoscritta alle circostanze di cui all'art. 9, par. 2, lett. a)²⁶ ovvero di cui alla successiva lett. g)²⁷ del GDPR²⁸.

Non può tacersi, tuttavia, come risulti amplificata, a fronte di un processo decisionale automatizzato, la tutela di taluni diritti dell'interessato, e

in particolare quello di essere informato e quello di accesso²⁹. Da un lato, infatti, il titolare del trattamento è tenuto a comunicare all'interessato l'esistenza di un processo decisionale basato in via esclusiva sul trattamento automatizzato, nonché a fornire «informazioni significative sulla logica utilizzata»³⁰ e a chiarire «l'importanza e le conseguenze previste di tale trattamento per l'interessato»³¹ e ciò a prescindere dal fatto che i dati personali siano raccolti presso l'interessato³² ovvero siano stati ottenuti non dall'interessato³³. Dall'altro, all'interessato è riconosciuto un diritto avente i medesimi contenuti dell'obbligo di informazione che grava sul titolare del trattamento e comprensivo, dunque, non soltanto della comunicazione dell'esistenza di un processo decisionale automatizzato, ma altresì delle informazioni sulla logica utilizzata dall'algoritmo, nonché sull'importanza e sulle conseguenze del trattamento per l'interessato³⁴.

26. E quindi ove «l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche ...».

27. E quindi ove «il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri ...».

28. Art. 22, par. 4. Cfr. anche d.lgs. n. 196/2003, come modificato dal d.lgs. n. 101/2018, artt. 2-*sexies*, 2-*septies*, 2-*octies*.

29. Nel senso di un'interpretazione necessariamente sistemica degli artt. 22 e 13-15 GDPR, v. MALGIERI-COMANDÉ 2017, p. 243 ss.

30. Pur non importando la comunicazione dell'algoritmo nella sua interezza, il riferimento alla «logica utilizzata» impone al titolare del trattamento di rendere note e facilmente comprensibili le motivazioni poste alla base della decisione.

31. Le *Linee guida sul processo decisionale automatizzato* sottolineano, peraltro, come la terminologia utilizzata indica che debbono «essere fornite informazioni sul trattamento previsto o futuro, nonché sulle possibili conseguenze del processo decisionale automatizzato sull'interessato», rilevando come «per rendere queste informazioni significative e comprensibili, dovrebbero essere forniti esempi reali e concreti del tipo di possibili effetti».

32. Cfr. art. 13, par. 2, lett. f).

33. Cfr. art. 14, par. 2, lett. g). Anche con riguardo a tale rinforzato diritto di essere informato sono previste eccezioni che possono distinguersi in relazione al «luogo» di raccolta e/o ottenimento dei dati: in questo senso, qualora i dati siano raccolti presso l'interessato, l'obbligo d'informazione non sussiste (soltanto) là dove quest'ultimo sia già in possesso delle informazioni (art. 13, par. 4); qualora, invece, i dati non siano stati ottenuti presso l'interessato, il ventaglio di circostanze idonee ad attenuare l'obbligo d'informazione risulta senz'altro più composito comprendendo, oltre a quella per cui l'interessato sia già in possesso delle informazioni, quelle per cui «la comunicazione risulta impossibile» o implica «uno sforzo sproporzionato», «l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato», «i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge» (art. 14, par. 5).

34. Cfr. art. 15, par. 1. Tale duplice configurazione è ben descritta in dottrina come «pretesa, giuridicamente riconosciuta e tutelata, alla conoscenza dell'esistenza di decisioni che ci riguardino prese da algoritmi e, correlativamente,

Al fine di garantire un controllo anche preventivo sul rispetto dei diritti e delle libertà dei soggetti interessati, il GDPR promuove il ricorso alle c.d. *privacy by design and by default*³⁵ e dunque alla valutazione d'impatto sulla protezione dei dati che il titolare del trattamento effettua prima di procedere al trattamento stesso là dove quest'ultimo presenta un elevato rischio per i diritti e le libertà delle persone fisiche³⁶, nonché al sistema di certificazioni, di sigilli e di marchi di protezione dei dati idonei a dimostrare la conformità al GDPR dei trattamenti effettuati dai titolari e dai responsabili del trattamento³⁷.

4. Il ricorso a decisioni automatizzate da parte della pubblica amministrazione nell'ordinamento italiano

I limiti da cui i dispositivi utilizzati nei processi di automatizzazione risultano spesso affetti e al contempo i rischi cui essi espongono i diritti e le libertà³⁸ non ne hanno arginato o comunque rallentato la diffusione e a ben guardare l'avanzamento è inarrestabile³⁹ non soltanto nell'ambito delle relazioni tra privati, ma altresì nel rapporto tra consociati e potere pubblico⁴⁰.

Non fa eccezione a questo proposito l'ordinamento italiano ove esistono esempi concreti di ricorso da parte delle pubbliche amministrazioni a siffatti moduli procedurali, i quali peraltro hanno generato un consistente contezioso che ha contribuito all'emersione di indirizzi giurisprudenziali tuttora consolidati.

4.1. Dal funzionario *dominus* del procedimento alla soddisfazione attraverso l'algoritmo del principio di buon andamento

Va innanzitutto segnalata una significativa evoluzione nella giurisprudenza amministrativa circa il ruolo della c.d. rivoluzione digitale per la pubblica amministrazione e il suo sviluppo.

A questo proposito, secondo l'iniziale orientamento del giudice amministrativo di primo grado, l'utilizzo dello strumento informatico in sede procedimentale deve porsi in una «posizione necessariamente servente» rispetto al procedimento stesso, risultando del tutto inammissibile che «l'ordinato svolgimento dei rapporti tra privato e Pubblica Amministrazione e fra Pubbliche

come dovere da parte di chi tratta i dati in maniera automatizzata, di porre l'interessato a conoscenza», così SIMONCINI 2019, p. 78.

35. Cfr. art. 25 GDPR. In particolare, in esecuzione della prima (“protezione dei dati fin dalla progettazione”), il titolare del trattamento è chiamato a prevenire il verificarsi di rischi per la protezione dei dati già nella fase della progettazione del sistema e dunque in una fase antecedente rispetto all'inizio del trattamento. In esecuzione della seconda (“protezione per impostazione predefinita”), il titolare del trattamento è chiamato a trattare soltanto i dati personali necessari e sufficienti per le finalità del trattamento e per il periodo strettamente necessario al raggiungimento delle medesime finalità. Entrambe trovano fondamento sul *risk based approach* (valutazione del rischio) idoneo a determinare (*rectius*, a meglio quantificare) la responsabilità del titolare o del responsabile del trattamento nella tutela dei diritti e delle libertà degli utenti (sulla valutazione del rischio v. anche considerando nn. 75 e 76 GDPR). Nell'ottobre 2020 l'*European Data Protection Board* ha pubblicato le linee guida sulla *Data protection by design e by default*.

36. Cfr. art. 35 GDPR.

37. Cfr. art. 42 GDPR.

38. Salvi i riferimenti documentali e bibliografici di cui si dirà, in generale, sulla non neutralità degli algoritmi e sui rischi derivanti da un capitalismo algoritmico v. BODEI 2019.

39. E che di avanzamento si tratti lo si deduce agevolmente anche dall'attenzione che taluni documenti europei dedicano al necessario sviluppo dei sistemi di intelligenza artificiale nel settore pubblico: in questa direzione v. il settore “G” “I.A. nel settore pubblico” all'interno del *Piano coordinato sull'intelligenza artificiale* COM(2018) 795, nonché il punto 4.F. “Promuovere l'adozione dell'IA nel settore pubblico” all'interno del *Libro bianco sull'intelligenza artificiale* COM(2020) 65.

40. In generale, sull'impatto dell'intelligenza artificiale sul diritto pubblico e costituzionale, v. PERFETTI 2017, p. 457 ss.; CASONATO 2019, p. 101 ss.; STRADELLA 2019; SIMONCINI-SUWEIS 2019, p. 87 ss.; CASONATO 2020; PAJNO-DONATI-PERRUCCI 2022; RINALDI 2022, p. 201 ss.; CORNELI 2023, p. 41 ss.; SIMONCINI 2023, p. 1 ss.; LALLI 2024.

Amministrazioni» possa in qualche modo risultare «ostacolato» da problematiche tecniche⁴¹. In un primo tempo, infatti, è stato ritenuto non conforme alla normativa in tema di procedimento amministrativo e all'art. 97 Cost. «affidare all'attivazione di meccanismi e sistemi informatici e al conseguente loro impersonale funzionamento, il dipanarsi di procedimenti amministrativi, sovente incidenti su interessi, se non diritti, di rilievo costituzionale, che invece postulano, onde approdare al corretto esito provvedimentale conclusivo, il disimpegno di attività istruttoria, acquisitiva di rappresentazioni di circostanze di fatto e situazioni personali degli interessati destinatari del provvedimento finale, attività, talora ponderativa e comparativa di interessi e conseguentemente necessariamente motivazionale, che solo l'opera e l'attività dianoetica dell'uomo può svolgere». Del resto, anche nell'ipotesi in cui raggiungano il maggior livello di precisione, se non addirittura la perfezione, le procedure informatiche «non poss[o]no mai soppiantare, sostituendola davvero appieno, l'attività cognitiva, acquisitiva e di giudizio che solo un'istruttoria affidata ad un funzionario persona fisica è in grado di svolgere»: quest'ultimo, dunque, «al fine di assicurare l'osservanza degli istituti di partecipazione, di interlocuzione procedimentale, di acquisizione degli apporti collaborativi del privato e degli interessi coinvolti nel procedimento, deve seguitare ad essere il *dominus* del procedimento stesso, all'uopo dominando le stesse procedure informatiche predisposte in funzione servente e alle quali va dunque riservato tutt'oggi un ruolo

strumentale e meramente ausiliario in seno al procedimento amministrativo e giammai dominante o surrogatorio dell'attività dell'uomo; ostando alla deleteria prospettiva orwelliana di dismissione delle redini della funzione istruttoria e di abdicazione a quella provvedimentale, il presidio costituito dal baluardo dei valori costituzionali scolpiti negli artt. 3, 24, 97 della Costituzione oltre che all'art. 6 della Convenzione europea dei diritti dell'uomo»⁴².

Tale orientamento è stato in certo senso superato con due pronunce, piuttosto note, del Consiglio di Stato, il quale salda fortemente il miglioramento della qualità dei servizi resi agli utenti con un sempre maggiore livello di digitalizzazione dell'amministrazione⁴³. Il giudice amministrativo di secondo grado, infatti, sottolinea, «gli indiscutibili vantaggi derivanti dalla automazione del processo decisionale dell'amministrazione mediante l'utilizzo di una procedura digitale ed attraverso un "algoritmo" [...] che in via informatica sia in grado di valutare e graduare una moltitudine di domande»⁴⁴. È del resto il principio costituzionale di buon andamento, secondo le tradizionali declinazioni dell'efficienza e dell'economicità, a imporre all'amministrazione di conseguire le proprie finalità «con il minor dispendio di mezzi e risorse e attraverso lo snellimento e l'accelerazione dell'iter procedimentale».

Tali opportunità, peraltro, non riguardano soltanto l'attività amministrativa vincolata, con riferimento alla quale certamente «il ricorso a strumenti di automazione della raccolta e valutazione dei dati» risulta ben più rilevante, potendo anche «l'esercizio di attività discrezionale, in specie

41. In questo senso TAR Lazio (Roma), Sez. III *bis*, n. 8902/2018.

42. TAR Lazio (Roma), Sez. III *bis*, nn. 9224, 9225, 9226, 9227, 9228, 9229, 9230/2018. La fattispecie concreta da cui tali pronunce prendevano le mosse ha riguardato l'applicazione che il Ministero dell'Istruzione, dell'Università e della Ricerca aveva fatto delle disposizioni contenute all'art. 1, co. 95 ss., l. 13 luglio 2015, n. 107 (c.d. "Buona scuola") relative a un piano straordinario di reclutamento a tempo indeterminato di personale docente per le istituzioni scolastiche statali di ogni ordine e grado. Le controversie, in particolare, hanno riguardato l'utilizzo, ai fini dell'assunzione e dell'effettiva presa di servizio nelle sedi scolastiche, di un algoritmo ignoto nelle modalità di funzionamento e all'esito del quale i trasferimenti disposti non hanno tenuto conto delle preferenze espresse in sede di presentazione delle domande: in altri termini, i ricorrenti di primo grado, pur in presenza di posti disponibili nelle province di residenza ovvero comunque nelle province prescelte, sono stati destinati in diverse e lontane province, assistendo al contempo all'assegnazione delle sedi ambite ad altri docenti collocatisi in posizione peggiore nella graduatoria di merito.

43. Il riferimento è a Sez. VI, nn. 2270 e 8472/2019 con cui il Consiglio di Stato è stato adito per riformare le sentenze pronunciate dal TAR Lazio (Roma) sull'applicazione della richiamata legge n. 107/2015. L'apparato motivazionale della sentenza n. 8472/2019 è stato successivamente riproposto dalla Sezione nella pronuncia n. 881/2020.

44. Consiglio di Stato, Sez. VI, n. 2270/2019.

tecnica, [...] in astratto beneficiare delle efficienze e, più in generale, dei vantaggi offerti dagli strumenti» in argomento⁴⁵: essendo entrambe manifestazione di attività autoritativa posta in essere per il conseguimento dell'interesse pubblico, sia quella vincolata che quella discrezionale ben possono fruire dell'automazione del processo decisionale⁴⁶.

Da un lato, infatti, il ricorso a decisioni automatizzate, coniugando il minor dispendio di risorse umane e strumentali a una sicura semplificazione del procedimento amministrativo, soddisfa senz'altro, come detto, il principio di cui all'art. 97, comma 2, Cost. sotto i profili dell'efficienza e dell'economicità.

Dall'altro lato, l'algoritmo, in quanto idoneo a eliminare «interferenze dovute a negligenza (o peggior dolo) del funzionario (essere umano)»⁴⁷, garantisce, altresì, l'imparzialità dell'amministrazione: nel processare numerose istanze con l'impiego di regole predeterminate, lo strumento elettronico e non manuale può meglio realizzare un intervento amministrativo neutrale poiché, facendo ricorso ad «asettici calcoli razionali basati su dati», riesce a «correggere le storture e le imperfezioni che caratterizzano tipicamente i processi cognitivi e le scelte compiute dagli esseri umani, messi in luce soprattutto negli ultimi anni da un'imponente letteratura di economia comportamentale e psicologia cognitiva»⁴⁸.

4.2. Le categorie tradizionali del diritto pubblico quale ineludibile lente di osservazione

La schietta apertura all'ingresso e all'utilizzo di strumenti informatici da parte del decisore pubblico non ha impedito, tuttavia, al Consiglio di Stato di rilevare come le determinazioni cui essi pervengono siano spesso tutt'altro che neutre⁴⁹.

Efficacemente il Collegio ha affermato che «l'adozione di modelli predittivi e di criteri in base ai quali i dati sono raccolti, selezionati, sistematizzati,

ordinati e messi insieme, la loro interpretazione e la conseguente formulazione di giudizi sono tutte operazioni frutto di precise scelte e di valori, consapevoli o inconsapevoli»: gli strumenti informatici, in altri termini, effettuano delle scelte utilizzando dati e criteri in relazione ai quali non sempre è assicurata la necessaria trasparenza.

E proprio la presenza di tali rischi impone di utilizzare quale lente di osservazione del fenomeno le categorie tradizionali del diritto pubblico, essendo queste necessarie ai fini dell'identificazione delle garanzie minime a tutela del singolo.

In questo senso, l'algoritmo è un atto amministrativo informatico: «la regola tecnica che governa ciascun algoritmo resta pur sempre una regola amministrativa generale, costruita dall'uomo e non dalla macchina, per essere poi (solo) applicata da quest'ultima [...]», cosicché l'utilizzo di procedure «robotizzate» non può determinare la violazione dei principi posti dall'ordinamento a fondamento dell'attività amministrativa. La regola algoritmica, benché espressa in forma matematica, ha «una piena valenza giuridica e amministrativa» e in quanto tale deve conformarsi ai principi generali dell'attività amministrativa, non potendo peraltro «lasciare spazi applicativi discrezionali [...], ma [dovendo] prevedere con ragionevolezza una soluzione definita per tutti i casi possibili, anche i più improbabili [...]»: l'esercizio della discrezionalità amministrativa, pertanto, non può riguardare la fase procedimentale materialmente svolta dallo strumento digitale, ma in via esclusiva la fase a essa immediatamente precedente e che consiste nell'elaborazione dello strumento stesso. A ciò si aggiunga, poi, l'irriducibile necessità che l'amministrazione – da intendersi quale funzionario-persona fisica – svolga «un ruolo *ex ante* di mediazione e composizione di interessi, anche per mezzo di costanti test, aggiornamenti e modalità di perfezionamento dell'algoritmo [...]» e al contempo che il giudice sia messo nelle condizioni

45. Consiglio di Stato, Sez. VI, n. 8472/2019.

46. Sul rilievo tra attività amministrativa vincolata e discrezionale nella materia che occupa v. VIOLA 2018, p. 22 ss.; VACCARI 2019, spec. parr. 4, 5 e 6.

47. Così Consiglio di Stato, Sez. VI, n. 2270/2019.

48. Così Consiglio di Stato, Sez. VI, n. 8472/2019.

49. Sulla necessità di una algoretica e dunque di una etica degli algoritmi v. CELOTTO 2020.

di sindacare *ex post* la correttezza della procedura automatizzata⁵⁰.

Il ricorso all'algoritmo, allora, non è nient'altro che un «modulo organizzativo», uno «strumento procedimentale ed istruttorio» su cui si instaurano le verifiche proprie di ogni procedimento amministrativo e il cui utilizzo non è da circoscrivere alla sola attività amministrativa vincolata a (s)vantaggio di quella discrezionale: benché il ricorso a strumenti informatici possa sembrare, per così dire, più piano con riguardo alla prima, come già anticipato, non può escludersi che i fini di pubblico interesse individuati dalla legge attributiva del potere ben possano essere perseguiti per il tramite di un algoritmo informatico anche in esercizio di attività espressione di discrezionalità amministrativa⁵¹.

5. La posizione del destinatario finale del provvedimento e il diritto effettivo di difesa in giudizio nella giurisprudenza amministrativa

A questo punto dell'indagine è necessario porre l'attenzione sulla posizione giuridica del destinatario del provvedimento e dunque sulle garanzie che devono essere offerte affinché esso possa effettivamente esercitare il proprio diritto a difendersi in giudizio, posto che l'opzione dell'amministrazione per l'algoritmo, in funzione servente all'attività umana ovvero decisionale, non può in ogni caso dare luogo a un abbassamento delle tutele apprestate ai singoli dalla legge sul procedimento amministrativo⁵².

A tale proposito la giurisprudenza amministrativa ha valorizzato in particolare gli elementi (i) della conoscibilità e della comprensibilità del modulo utilizzato e dei criteri applicati; (ii) dell'imputabilità della decisione all'organo titolare del potere, il quale deve essere in condizione di esercitare il proprio controllo sulle modalità

attraverso cui l'elaborazione è condotta e sull'esito cui l'algoritmo perviene; (iii) del carattere non discriminatorio dell'algoritmo; (iv) della sindacabilità da parte del giudice amministrativo⁵³.

In ipotesi di decisione automatizzata assunta da un'amministrazione pubblica, viene in considerazione l'art. 42 della Carta dei diritti fondamentali dell'Unione europea e del *right to a good administration* in esso contenuto, cosicché ove la p.a. «intende adottare una decisione che può avere effetti avversi su di una persona, essa ha l'obbligo di sentirla prima di agire, di consentirle l'accesso ai suoi archivi e documenti, ed, infine, ha l'obbligo di «dare le ragioni della propria decisione»⁵⁴.

5.1. L'accessibilità e la comprensibilità della formula tecnica che si traduce in regola giuridica

In primo luogo, le modalità attraverso cui si perviene alla decisione automatizzata devono essere conoscibili e comprensibili. Questa garanzia, consentendo di tradurre una «formula tecnica» in una «regola giuridica», deve riguardare «da[gli] autori [dell'algoritmo] al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti» e ciò al fine di verificare la rispondenza dell'output a quanto stabilito dalla fonte legislativa ovvero dall'amministrazione procedente⁵⁵.

L'algoritmo che venga a esprimere lo svolgimento dell'attività dell'amministrazione pubblica rimane dunque assoggettato alle norme in materia di accesso agli atti e ai documenti amministrativi e ciò a prescindere dalla natura pubblica o privata del soggetto che fornisce il programma informatico⁵⁶. È, infatti, da considerarsi certamente recessivo l'interesse alla riservatezza dell'impresa produttrice dell'algoritmo, la quale non può che sopportare,

50. Sul punto NICOTRA-VARONE 2019, p. 86 ss. e spec. 99 ss.

51. Ancora Consiglio di Stato, n. 8472/2019.

52. Su questo tema, e in particolare sull'esistenza di una «riserva di umanità», quale nocciolo duro di presenza umana che è necessario garantire nell'esercizio delle funzioni amministrative, v. il recente volume di GALLONE 2023.

53. Consiglio di Stato, Sez. IV, n. 5117/2023 (cfr. punto 10.10).

54. Consiglio di Stato, Sez. VI, n. 8472/2019; in senso conforme v. anche Consiglio di Stato, Sez. VI, n. 881/2020; TAR Campania (Napoli), Sez. III, n. 7003/2022.

55. Cfr. Consiglio di Stato, Sez. VI, n. 2270/2019.

56. V. TAR Lazio (Roma), Sez. III, 1° luglio 2020, n. 7526.

per così dire, il peso derivante dagli obblighi di trasparenza cui sono sottoposte le autorità pubbliche con cui intrattiene rapporti contrattuali⁵⁷. Al soggetto che ha ideato l'algoritmo, tuttavia, va riconosciuta la qualità di parte controinteressata all'ostensione nel processo amministrativo, posto che l'accesso a dati personali e/o a segreti tecnici o commerciali può comportare un pregiudizio nella propria sfera giuridica⁵⁸.

La decisione è dunque chiamata a rispondere a un duplice obbligo: quello «di indicare quale sia stato il meccanismo informatico di decisione impiegato (c.d. conoscibilità)», nonché quello «di spiegare il suo funzionamento in termini comprensibili per l'utente non dotato di competenze tecniche (c.d. comprensibilità)». Diversamente, le garanzie processuali di cui agli artt. 24 e 113 Cost. non possono che risultare frustrate dalla non intellegibilità della regola giuridica sottesa al processo automatizzato, non essendo per questa via consentito dapprima all'interessato e in un secondo momento al giudice cogliere lo sviluppo logico e giuridico che ha condotto l'amministrazione a provvedere⁵⁹.

5.2. L'imputabilità della decisione e della relativa responsabilità all'organo titolare del potere

L'imputabilità della scelta finale al soggetto titolare del potere autoritativo e individuato sulla base del principio di legalità è poi funzionale all'individuazione del funzionario-persona fisica responsabile dell'azione amministrativa e segue alla verifica da parte di quest'ultimo della legittimità degli esiti dell'elaborazione condotta dall'algoritmo

conformemente al principio di non esclusività della decisione automatizzata⁶⁰.

Chi subisce gli effetti giuridici di una decisione automatizzata «ha il diritto a che tale decisione non sia basata unicamente sul processo automatizzato, affidando al funzionario responsabile il compito di controllare, e quindi validare o, al contrario, smentire la decisione automatica». Per quanto la tecnologia possa contribuire al miglioramento, anche qualitativo, del processo decisionale, si è, infatti, imposta «un'opposta esigenza che controbilancia le spinte semplificatorie e acceleratorie, ovvero quella di assicurare un controllo umano del procedimento, in funzione di garanzia (c.d. *human in the loop*) in modo che il funzionario possa in qualsiasi momento intervenire per compiere interlocuzioni con il privato, per verificare a monte l'esattezza dei dati da elaborare, mantenendo il costante controllo del procedimento»⁶¹.

Ciò, peraltro, consente di ridimensionare il rischio autorevolmente messo in luce in dottrina e relativo alla circostanza per cui «facendo uso della decisione robotica, l'amministrazione scarica sul giudice il proprio ruolo di "mediazione" degli interessi, di valutazione e talvolta di accertamento del fatto» e ciò in quanto «il giudice, nell'accertare la correttezza dell'algoritmo [...] può dover svolgere, per la prima volta sul piano "umano", valutazioni ed accertamenti fatti direttamente in via automatica»⁶². La predisposizione di appositi momenti di interlocuzione tra uomo e macchina non può che favorire forme di verifica *ex ante* e per tale via contenere il c.d. effetto performativo, in forza del quale la decisione amministrativa verrebbe diversamente a coincidere con l'algoritmo stesso «che da mero presupposto tecnico assurge ad elemento fondante ed esclusivo»⁶³.

57. Sul software quale opera dell'ingegno e sulla necessaria ostensione dei codici sorgente dell'algoritmo in cui si sostanzia lo stesso procedimento, v. diffusamente TAR Lazio (Roma), Sez. III *bis*, 22 marzo 2017, n. 376. In proposito, CAVALLARO-SMORTO 2019, p. 12 ss.

58. In questo senso Consiglio di Stato, Sez. VI, n. 30/2020.

59. TAR Campania (Napoli), Sez. III, 14 novembre 2022, n. 7003.

60. Nella procedura decisionale deve esistere «un contributo umano capace di controllare, validare ovvero smentire la decisione automatica. In ambito matematico ed informativo il modello viene definito come HITL (*human in the loop*), in cui, per produrre il suo risultato è necessario che la macchina interagisca con l'essere umano» (Consiglio di Stato, Sez. VI, n. 8472/2019). Sul tema v. MARCHETTI 2021, p. 367 ss.; DI CIOMMO 2023, p. 71 ss.; GALETTA 2023; MARTIRE 2024.

61. TAR Campania (Napoli), Sez. III, 14 novembre 2022, n. 7003.

62. In tal senso PATRONI GRIFFI 2018, pp. 4-5.

63. Così DALFINO 2020, par. 4.

L'individuazione, attraverso la legge che attribuisce il potere, di un centro di imputazione e di responsabilità è dunque del tutto necessaria e strumentale alla verifica della logicità e della legittimità della decisione automatizzata, non essendo «le norme tradizionali [...] sufficienti per attivare la responsabilità per i danni causati da un robot, in quanto non consent[on]o di determinare qual è il soggetto cui incombe la responsabilità del risarcimento né di esigere da tale soggetto la riparazione dei danni causati»⁶⁴.

5.3. Il carattere non discriminatorio dell'algoritmo

Dal considerando n. 71 del GDPR è fatto, poi, derivare un ulteriore principio, di non discriminazione algoritmica, in base al quale l'algoritmo non soltanto deve essere conoscibile e comprensibile e deve dare luogo a un esito su cui vi è stato intervento umano, ma altresì non deve produrre effetti discriminatori sui destinatari della decisione sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale⁶⁵.

Il titolare del trattamento è chiamato a utilizzare «procedure matematiche o statistiche appropriate per la profilazione, mettendo in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali, secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i

diritti dell'interessato e che impedisca tra l'altro effetti discriminatori ovvero che comportano misure aventi tali effetti»: in tali circostanze, è necessario «rettificare i dati in "ingresso" per evitare effetti discriminatori nell'output decisionale» e tale operazione presuppone l'intervento attivo del soggetto che assicura l'input alla macchina per generare l'output⁶⁶.

5.4. La sindacabilità da parte del giudice amministrativo

L'effettività del diritto di difesa, infine, passa anche attraverso la soggezione della regola algoritmica alla piena cognizione e al pieno sindacato del giudice amministrativo.

Se, infatti, già la conoscibilità della regola algoritmica è funzionale alla cognizione e al sindacato del giudice, il quale deve essere posto in condizione di valutare la correttezza del processo informatico e dunque la logicità e la ragionevolezza della decisione amministrativa robotizzata⁶⁷, costituisce declinazione diretta del diritto di cui all'art. 24 Cost. la possibilità di sottoporre a verifica di legittimità le modalità attraverso cui il potere è stato esercitato e si ripercuote, per il tramite di una decisione automatizzata, sulla sfera giuridica del destinatario del provvedimento.

La valutazione che il giudice pone in essere a valle dell'automazione del processo decisionale non può, allora, che essere del tutto affine a quella che esso effettua con riguardo al potere esercitato secondo i canoni tradizionali del diritto pubblico.

In questa misura, la conoscibilità dei dati e dello stesso algoritmo consente al sindacato del giudice di abbracciare il processo informatico nella sua

64. Consiglio di Stato, Sez. VI, n. 8472/2019.

65. Argomentando intorno alla regola della non esclusività della decisione algoritmica, infatti, il considerando n. 71 rileva che «[a]l fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e impedisca, tra l'altro, effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero un trattamento che comporti misure aventi tali effetti».

66. Consiglio di Stato, Sez. VI, n. 8472/2019.

67. Cfr. Consiglio di Stato, Sez. VI, n. 2270/2019. Nella più volte citata sentenza n. 8472/2019, il Collegio arricchisce le argomentazioni sulla conoscibilità dell'algoritmo con puntuali richiami agli artt. 13-14 e 15 del GDPR, dedicati rispettivamente, come innanzi rilevato, al diritto di informazione e al diritto di accesso degli interessati.

interezza e dunque il controllo sulla ragionevolezza della decisione amministrativa algoritmica⁶⁸.

6. Gli sviluppi più recenti in tema di intelligenza artificiale antropocentrica e affidabile nel Regolamento (UE) 2024/1689

Venendo agli algoritmi di intelligenza artificiale, i sicuri e irrinunciabili benefici e vantaggi a essi ricollegabili non hanno impedito di rilevare e stigmatizzare la non sufficiente centralità della persona fisica nel relativo funzionamento e quindi di porre l'attenzione sui consistenti rischi cui i diritti fondamentali dei singoli sono esposti.

Tali preoccupazioni e consapevolezze, rilevate anche in ambito convenzionale⁶⁹, oltre che nazionale⁷⁰, hanno orientato in una prospettiva *de iure condendo* i contenuti di numerosi recenti documenti europei e in questo senso possono essere richiamati almeno le *Norme di diritto civile sulla robotica*⁷¹, il parere di iniziativa del Comitato economico e sociale europeo *L'intelligenza artificiale — Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società*⁷², il *Piano coordinato sull'intelligenza artificiale*⁷³, *L'intelligenza artificiale per l'Europa*⁷⁴, *Creare fiducia nell'intelligenza artificiale antropocentrica*⁷⁵, sino al *Libro bianco*

68. Consiglio di Stato, Sez. VI, n. 2270/2029.

69. In ambito convenzionale si rammentano le *Linee-guida in materia di intelligenza artificiale e protezione dei dati* emanate il 25 gennaio 2019 dal Comitato consultivo della *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale*, sottoscritta a Strasburgo il 28 gennaio 1981 e ratificata in Italia con legge n. 98/1989 (c.d. Convenzione 108) all'interno delle quali la necessità di evitare il rischio di discriminazioni è contenuto nella parte dedicata agli sviluppatori, ai produttori e ai fornitori di servizi, in quella dedicata ai legislatori e ai policy makers.

70. Nell'ordinamento italiano, nondimeno, gli effetti discriminatori potenzialmente derivanti dai dispositivi intelligenti sono stati fortemente stigmatizzati. Cfr. in proposito il *Libro bianco sull'intelligenza artificiale al servizio del cittadino*, elaborato dalla *task force* istituita in seno all'Agenzia per l'Italia digitale e diffuso nel marzo 2018, che riconosce una delle sfide dell'intelligenza artificiale nella prevenzione delle disuguaglianze determinate (anche) da dati o algoritmi affetti da *bias* di tipo discriminatorio. È possibile, altresì, richiamare il documento *Proposte per una strategia italiana per l'intelligenza artificiale*, curato da un gruppo di esperti nominato dal Ministero per lo Sviluppo Economico e pubblicato nel luglio 2019, ove uno dei fili conduttori delle raccomandazioni adottate è proprio rinvenibile nel contrasto alle disuguaglianze e alle discriminazioni quali rischi connessi all'utilizzo non doloso dell'intelligenza artificiale.

71. *Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica 2015/2103* ove il Parlamento europeo sottolinea come il quadro etico di riferimento dovrebbe essere basato sui principi di cui all'art. 2 del TUE e sanciti all'interno della Carta dei diritti fondamentali dell'Unione europea.

72. Nel parere (2017/C 288/01) il CESE chiede «di introdurre un codice etico per lo sviluppo, la diffusione e l'utilizzo dell'IA, in modo tale che questi sistemi siano compatibili durante tutto il loro ciclo operativo con i principi della dignità umana, dell'integrità, della libertà, della privacy e della diversità culturale e di genere, nonché con i diritti umani fondamentali».

73. Il riferimento è alla Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni – [COM\(2018\) 795](#) – ove è posta in evidenza la necessità di perseguire l'etica sin dalla progettazione e di pervenire a un «quadro normativo adeguato, prevedibile ed etico fondato su efficaci misure di salvaguardia per la protezione dei diritti e delle libertà fondamentali».

74. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni – [COM\(2018\) 237](#) all'interno della quale è sottolineata l'esigenza di assicurare un quadro etico e giuridico adeguato, basato sui valori dell'Unione e coerente con la Carta dei diritti fondamentali dell'Ue.

75. Cfr. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni – [COM\(2019\) 168](#) – ove è ribadita l'urgenza di conseguire un'intelligenza artificiale *antropocentrica* attraverso il rispetto dei principi fondanti lo Stato di diritto.

sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia⁷⁶.

La promozione di un'intelligenza artificiale antropocentrica e affidabile a livello europeo acquista una dimensione normativa soltanto da ultimo con l'adozione del Regolamento (UE) 2024/1689, anche noto come *AI ACT*, pubblicato sulla *Gazzetta ufficiale dell'Unione europea* il 12 luglio 2024⁷⁷.

Il regolamento, pur considerando l'intelligenza artificiale una tecnologia che contribuisce al conseguimento di considerevoli benefici a livello economico, ambientale e sociale nelle attività industriali e sociali⁷⁸, rileva sin da subito come essa possa comportare rischi e pregiudizi, materiali e immateriali⁷⁹. E proprio in ragione dell'impatto che tale tecnologia ha sulla società, l'Unione ritiene necessario sviluppare un quadro giuridico di regole armonizzate al fine di promuovere lo sviluppo, l'utilizzo e l'adozione di sistemi intelligenti nel mercato interno, «garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e

la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione»⁸⁰.

Non essendo qui possibile offrire un'analisi sistematica dei contenuti del Regolamento sull'intelligenza artificiale, nell'economia del presente lavoro pare il caso di sottolineare innanzitutto due aspetti.

Il primo è che, ai sensi del combinato disposto di cui agli artt. 2 e 3, esso si applica anche alle autorità pubbliche situate all'interno dell'Unione che utilizzino un sistema di intelligenza artificiale⁸¹, definito come «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali»⁸².

Il secondo attiene al fatto che l'obiettivo dell'intervento regolamentare è la protezione dei diritti sanciti dalla Carta dei diritti fondamentali dell'Unione europea⁸³, compresi dunque il diritto a una buona amministrazione⁸⁴ e quello di difesa⁸⁵.

Seguendo un *risk based approach*⁸⁶, il regolamento identifica pratiche vietate di intelligenza artificiale⁸⁷, sistemi di intelligenza artificiale “ad alto

76. [COM\(2020\) 65](#) ove la Commissione persegue il duplice obiettivo di promuovere l'adozione dell'intelligenza artificiale e di affrontare i rischi associati a determinati utilizzi di questa nuova tecnologia.

77. Regolamento del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

78. Considerando 4.

79. Considerando 5.

80. Art. 1.

81. Secondo l'art. 2, infatti, il regolamento si applica «b) ai *deployer* dei sistemi di IA che hanno il loro luogo di stabilimento o sono situati all'interno dell'Unione». Il successivo art. 3 invece definisce “*deployer*” «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale».

82. Art. 3, par. 1, n. 1.

83. Per un primo approfondimento sul tema v. MANCIOPPI 2024, p. 112 ss.

84. Art. 41 CDFUE.

85. Art. 47 ss. CDFUE.

86. All'art. 3, par. 1, n. 2 è definito “rischio” «la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso».

87. Capo II.

rischio⁸⁸, specifici sistemi di intelligenza artificiale per i quali sono indicati taluni obblighi di trasparenza in capo a fornitori e *deployers*⁸⁹ e modelli di intelligenza artificiale per finalità generali⁹⁰.

Poiché è proprio il potenziale impatto negativo sui diritti fondamentali tutelati nella Carta di Nizza ad assumere centrale rilevanza ai fini della classificazione di un sistema di IA tra quelli c.d. «ad alto rischio»⁹¹, pare opportuno proporre su questi ultimi un approfondimento, tenendo presente che essi, elencati all'interno dell'allegato III del Regolamento, appaiono *ictu oculi* ben poter essere strumentali all'esercizio delle funzioni e all'erogazione dei servizi pubblici⁹².

A questo proposito, la normativa europea prevede che tali sistemi debbano essere conformi a taluni requisiti e introduce un apposito sistema di gestione dei rischi, definito come «un processo iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio, che richiede un riesame e un aggiornamento costanti e sistematici»⁹³.

Si stabilisce, infatti, che i sistemi ad alto rischio siano sviluppati sulla base di set di dati di addestramento, convalida e prova che soddisfino criteri di

qualità⁹⁴; già prima dell'immissione sul mercato o della messa in servizio, siano accompagnati da una documentazione tecnica idonea a dimostrarne la conformità ai requisiti previsti dal regolamento stesso⁹⁵ e a consentire la registrazione automatica degli eventi per la durata del ciclo di vita del sistema⁹⁶; siano progettati e sviluppati al fine di garantire trasparenza e di assicurare la possibilità di interpretazione dell'output da parte del *deployer*, nonché il suo l'utilizzo adeguato⁹⁷; siano, altresì, progettati e sviluppati, «anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso»⁹⁸ e in modo da conseguire accuratezza, robustezza e ciphersicurezza durante tutto il loro ciclo di vita⁹⁹.

Sicuro rilievo assume, poi, la previsione per cui, prima di utilizzare un sistema di intelligenza artificiale ad alto rischio¹⁰⁰, i *deployers* che siano organismi di diritto pubblico ovvero enti privati che forniscono servizi pubblici sono chiamati a effettuare una *valutazione d'impatto sui diritti fondamentali* che l'utilizzo del sistema può produrre¹⁰¹.

88. Capo III.

89. Capo IV.

90. Capo V.

91. Art. 6 ss.

92. All'interno dell'allegato III richiamato, infatti, tra i settori di applicazione dei sistemi di intelligenza artificiale ad alto rischio vi sono quelli dell'istruzione e della formazione professionale, dell'occupazione e della gestione dei lavoratori, dell'accesso e della fruizione di prestazioni e servizi pubblici, della migrazione, dell'asilo e della gestione del controllo delle frontiere, dell'amministrazione della giustizia e dei processi democratici.

93. Art. 9, par. 2.

94. Art. 10.

95. Art. 11.

96. Art. 12.

97. Cfr. art. 13. Il par. 2 precisa che «I sistemi di IA ad alto rischio sono accompagnati da istruzioni per l'uso, in un formato appropriato digitale o non digitale, che comprendono informazioni concise, complete, corrette e chiare che siano pertinenti, accessibili e comprensibili per i *deployer*».

98. Art. 14.

99. Art. 15.

100. A eccezione dei sistemi destinati a essere usati nel settore «Infrastrutture critiche: i sistemi di IA destinati a essere utilizzati come componenti di sicurezza nella gestione e nel funzionamento delle infrastrutture digitali critiche, del traffico stradale o nella fornitura di acqua, gas, riscaldamento o elettricità» di cui all'allegato III, punto 2.

101. Art. 27. Ai fini della valutazione i *deployers* tengono presenti i seguenti elementi: «a) una descrizione dei processi del *deployer* in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista; b) una descrizione del periodo di tempo entro il quale ciascun sistema di IA ad alto rischio è destinato a essere

Il regolamento, che individua puntualmente gli obblighi gravanti su fornitori, *deployers*, importatori e distributori di sistemi ad alto rischio¹⁰² e distribuisce «lungo la catena del valore dell'IA» le responsabilità dei soggetti variamente coinvolti nell'immissione sul mercato o nella messa in servizio del sistema stesso¹⁰³, disciplina nel dettaglio le procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e per il loro monitoraggio¹⁰⁴ e prevede l'istituzione, ai fini della registrazione dei sistemi di IA ad alto rischio, di un'apposita banca dati dell'Ue¹⁰⁵.

L'indagine può giovare di qualche ulteriore riferimento alla disciplina generale contenuta nel Regolamento.

Procedendo in questo senso, si rileva innanzitutto come l'*AI Act*, il quale peraltro disegna una vera e propria *governance* nel settore dell'intelligenza artificiale a livello europeo¹⁰⁶ e a livello nazionale¹⁰⁷, riconosca all'efficienza e alla qualità della pubblica amministrazione e dei servizi pubblici un ruolo di primo piano nella sperimentazione normativa di specifici sistemi di intelligenza artificiale nell'interesse pubblico¹⁰⁸.

Ancora, si evidenzia come alle autorità o agli organismi pubblici nazionali chiamati a controllare o garantire il rispetto degli obblighi derivanti dal

diritto europeo per la tutela dei diritti fondamentali in relazione all'uso dei sistemi di IA ad alto rischio sia consentito fare richiesta di «qualsiasi documentazione creata o mantenuta a norma del [...] regolamento o di accedervi, in una lingua e un formato accessibili, quando l'accesso a tale documentazione è necessario per l'efficace adempimento dei loro mandati entro i limiti della loro giurisdizione». Agli stessi, peraltro, ove tale documentazione non risulti sufficiente ad accertare l'eventuale violazione degli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali, è rimessa la possibilità di presentare all'autorità di vigilanza del mercato una richiesta motivata al fine di organizzare una prova del sistema di IA ad alto rischio mediante mezzi tecnici, la quale deve svolgersi con il coinvolgimento dell'autorità o dell'organismo pubblico che ne ha fatto richiesta¹⁰⁹.

Venendo ai mezzi di ricorso individuali, oltre al diritto riconosciuto in capo a qualsiasi persona fisica o giuridica di presentare un reclamo all'autorità di vigilanza del mercato in ipotesi di supposta violazione di quanto stabilito nel Regolamento¹¹⁰, l'art. 86 configura in capo al destinatario di una decisione adottata sulla base dell'output di un sistema di IA ad alto rischio – la quale produca effetti giuridici o in modo analogo incida significativamente

utilizzato e con che frequenza; c) le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico; d) i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati a norma della lettera c), del presente paragrafo tenendo conto delle informazioni trasmesse dal fornitore a norma dell'articolo 13; e) una descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso; f) le misure da adottare qualora tali rischi si concretizzino, comprese le disposizioni relative alla governance interna e ai meccanismi di reclamo». Ai sensi del par. 2, alla valutazione bisogna procedere al primo uso del sistema e al *deployer* è comunque consentito basarsi su valutazioni d'impatto effettuate in precedenza se del caso anche da un fornitore. In ogni caso, ove durante l'uso del sistema uno qualsiasi degli elementi elencati al paragrafo 1 sia cambiato o non sia più aggiornato, il *deployer* adotta le misure necessarie per aggiornare le informazioni.

102. Art. 16 ss.

103. Art. 25.

104. Capo III, Sezione IV.

105. Cfr. art. 49 e 71.

106. È prevista infatti l'istituzione di un Consiglio per l'IA, di un Forum consultivo e di un Gruppo di esperti scientifici indipendenti (cfr. artt. 64-69).

107. L'art. 70 prevede che ciascuno Stato membro istituisca o designi come autorità nazionali competenti almeno un'autorità di notifica e un'autorità di vigilanza del mercato.

108. V. in particolare art. 59, par. 1, lett. a), v).

109. Art. 77.

110. Art. 85.

su tale persona in un modo che essa ritenga avere un impatto negativo sulla salute, sulla sicurezza o sui diritti fondamentali – il diritto di ottenere dal *deployer* spiegazioni chiare e significative sul ruolo del sistema di IA nella procedura decisionale e sui principali elementi della decisione adottata.

7. Lo spazio di intervento del legislatore nazionale e la necessaria alfabetizzazione in tema di intelligenza artificiale. Considerazioni conclusive

Venendo a concludere, si propone qualche notazione finale su due aspetti.

Il primo attiene allo spazio che residua in capo al legislatore nazionale per disciplinare l'utilizzo da parte della pubblica amministrazione di strumenti informatici al fine di decidere¹¹¹. E, a questo proposito, pare potersi distinguere a seconda che la decisione si avvalga di un algoritmo, per così dire, tradizionale, per quanto automatizzato, ovvero di un algoritmo di intelligenza artificiale.

Con riguardo agli algoritmi tradizionali, infatti, una disciplina legislativa interna che, nell'ambito degli spazi rimessi in particolare dall'art. 22 GDPR¹¹², introduca norme in materia di procedimento amministrativo automatizzato, potrebbe rivelarsi (ancora) opportuna¹¹³, oltre che utile sia per l'esercizio del diritto di difesa che per l'attività di accertamento compiuta dal giudice amministrativo. Tale intervento legislativo dovrebbe individuare quantomeno le tipologie di attività amministrativa per le quali è consentito il ricorso a tale modulo procedimentale, l'organo competente a definire i criteri per la traduzione della regola giuridica in formula tecnica, le modalità e i tempi per l'esercizio di un regolare controllo da

parte del funzionario-persona fisica sul corretto funzionamento del sistema informatico utilizzato, meccanismi *ad hoc* idonei ad adattare le peculiarità procedurali ai principi di trasparenza e partecipazione e ad assolvere gli oneri motivazionali, chiare forme di imputazione della responsabilità non soltanto nel rapporto tra amministrazione e destinatario del provvedimento, ma anche tra amministrazione e soggetto terzo titolare della proprietà intellettuale dell'algoritmo e ancora, al fine di «evitare che si possano “mascherare” pericolosi sviamenti di potere celati dietro il “velo” della tecnica»¹¹⁴, specifiche «cautele pubblicistiche» nella fase dell'appalto di servizi che riguarda la scelta dell'aggiudicatario per l'elaborazione del software e per la realizzazione del relativo algoritmo.

Con riferimento invece agli algoritmi di intelligenza artificiale, l'introduzione di un modello di verifica di conformità a requisiti predeterminati e di valutazione d'impatto sui diritti fondamentali, spostando in una fase preventiva l'*accreditamento* dei sistemi di intelligenza artificiale di cui l'autorità pubblica può avvalersi, senza peraltro omettere di prevedere momenti di ulteriore ed eventuale esame a valle dell'output, pare invece ridurre sensibilmente gli spazi per un intervento legislativo interno. Qualche conferma in questo senso parrebbe derivare dai contenuti dell'art. 13 (*Uso dell'intelligenza artificiale nella pubblica amministrazione*) del d.d.l. A.S. 1146 recante *Disposizioni e delega al Governo in materia di intelligenza artificiale*¹¹⁵, il quale si limita a funzionalizzare il ricorso a sistemi intelligenti all'incremento dell'efficienza amministrativa e al miglioramento della qualità dei servizi erogati, nella garanzia della conoscibilità del funzionamento e della tracciabilità del suo utilizzo

111. Sul ruolo della “mediazione giuridica” tra la tecnologia e l'impatto sociale delle funzioni svolte dalla macchina v. RESTA 2019, p. 199 ss. e spec. p. 233. Sulla non neutralità degli algoritmi quale fondamento della necessità di un intervento normativo v. GIORGINI 2019, p. 131 ss. e spec. p. 145 ss.

112. Come visto, la disposizione prevede, tra le ipotesi di deroga al divieto di decisione basata unicamente sul trattamento automatizzato, quella per la quale la decisione stessa «sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato».

113. Sulla necessità che il potere di emanare una decisione automatizzata sia conferito con legge v. diffusamente CIVITARESE MATTEUCCI 2019, p. 5 ss.

114. Così VACCARI 2019, par. 7.

115. Presentato dalla Presidente del Consiglio dei ministri, on. Giorgia Meloni, e dal Ministro della giustizia, on. Carlo Nordio, il 20 giugno 2024 e attualmente in [trattazione in Commissione](#).

e nel rispetto dell'autonomia e del potere decisionale del funzionario quale unico responsabile del procedimento e del provvedimento amministrativo. In regime di invarianza finanziaria, poi, il d.d.l. prevede che le amministrazioni adottino misure tecniche, organizzative e formative al fine di garantire un utilizzo responsabile dell'intelligenza artificiale e di sviluppare capacità trasversali degli utilizzatori. E appaiono in questo senso coerenti gli obiettivi che la *Strategia Italiana per l'Intelligenza Artificiale 2024-2026*¹¹⁶ indica nella sezione specificamente dedicata alla pubblica amministrazione e che, guardando alle tecnologie dell'intelligenza artificiale per supportare i processi amministrativi e favorire la fruizione dei servizi della pubblica amministrazione per cittadini e imprese, parrebbero, unitamente alle azioni strategiche all'uopo individuate¹¹⁷, *accompagnare*, più che orientare, la graduale futura applicazione del Regolamento (UE) 2024/1689¹¹⁸.

Il secondo aspetto attiene al tema della c.d. alfabetizzazione in materia di intelligenza artificiale definita dall'*AI Act* come «le competenze, le conoscenze e la comprensione che consentono ai fornitori, ai *deployer* e alle persone interessate, tenendo conto dei loro rispettivi diritti e obblighi nel contesto del presente regolamento, di procedere a una diffusione informata dei sistemi di IA, nonché di acquisire consapevolezza in merito alle opportunità e ai rischi dell'IA e ai possibili danni che essa

può causare»¹¹⁹. Per il conseguimento di essa, il Regolamento demanda a fornitori e *deployers* il compito di adottare idonee «misure per garantire nella misura del possibile un livello sufficiente di alfabetizzazione in materia di IA» del personale, partendo dalla relativa conoscenza tecnica, esperienza, istruzione e formazione¹²⁰.

Con riguardo a tale questione, pare sicuramente intercettato dalla *Strategia italiana* richiamata il necessario irrobustimento competenziale degli apparati amministrativi, non più rinviabile per un'amministrazione che intenda o comunque sia chiamata ad avvalersi di strumenti tecnologici. Il raggiungimento di tale obiettivo non può che passare tuttavia attraverso specifici investimenti, non essendo seriamente percorribile optare per la ormai nota espressione «con le risorse finanziarie, umane e strumentali disponibili a legislazione vigente» che pure al momento in cui si scrive risulta nell'art. 13, comma 4 del d.d.l. n. 1146.

In definitiva, si mostra come ineludibile la sfida per le università di offrire nuovi percorsi universitari, post-universitari e formativi che, coniugando saggiamente (quantomeno) scienze giuridiche e informatiche in un'ottica interdisciplinare¹²¹, siano in grado di creare nuove professionalità e competenze attraverso le quali affrontare le sfide che l'incontro tra sistemi intelligenti e diritto in generale e diritto pubblico in particolare impongono¹²².

116. Il testo, elaborato da un Comitato di esperti per supportare il Governo nella definizione di una normativa nazionale e delle politiche sull'IA, è stato pubblicato sul sito web dell'Agenzia per l'Italia digitale il 22 luglio 2024.

117. Sono sei le azioni strategiche previste: linee guida per promuovere l'adozione dell'IA; linee guida per il procurement; linee guida per la realizzazione di applicazioni di IA; semplificazione per cittadini e imprese; efficientamento della PA; IA nelle scuole per la PA.

118. L'art. 113 dell'*AI Act*, infatti, fissa al ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea l'entrata in vigore del Regolamento e a decorrere dal 2 agosto 2026 la relativa applicazione. Ai sensi del par. 3, poi, «Tuttavia: a) I capi I e II si applicano a decorrere dal 2 febbraio 2025; b) Il capo III, sezione 4, il capo V, il capo VII, il capo XII e l'articolo 78 si applicano a decorrere dal 2 agosto 2025, ad eccezione dell'articolo 101; c) L'articolo 6, paragrafo 1, e i corrispondenti obblighi di cui al presente regolamento si applicano a decorrere dal 2 agosto 2027».

119. Art. 3, par. 1, n. 56.

120. Art. 4.

121. Sull'opportunità di rimodulare la formazione dei giuristi nelle università, v. GALETTA-CORVALÁN 2019, p. 3.

122. Sui mutamenti che la professione legale è destinata a conoscere nel futuro prossimo v. SUSSKIND 2019.

Riferimenti bibliografici

- G. AIRENTI, B.G. BARA (1978), *Intelligenza artificiale*, FrancoAngeli, 1978
- E. ANGNER (2017), *Economia comportamentale. Guida alla teoria della scelta*, Hoepli, 2017
- R. BODEI (2019), *Dominio e sottomissione. Schiavi, animali, macchine*, *Intelligenza Artificiale*, il Mulino, 2019
- M. BOZZO (1996), *La grande storia del computer. Dall'abaco all'intelligenza artificiale*, Dedalo, 1996
- G. BUSIA, L. LIGUORI, O. POLLICINO (2016), *Le nuove frontiere della privacy nelle tecnologie digitali: bilanci e prospettive*, Aracne, 2016
- L. CARLUCCI AIELLO, M. CIALDEA MAYER (1995), *Invito all'intelligenza artificiale*, FrancoAngeli, 1995
- C. CASONATO (2020), *Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro*, in "Consulta online - Liber amicorum per Pasquale Costanzo", 13 gennaio 2020
- C. CASONATO (2019), *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in "Diritto pubblico comparato ed europeo", Speciale 2019
- M.C. CAVALLARO, G. SMORTO, (2019), *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in "federalismi.it", 2019, n. 16
- R. CAVALLO PERIN (a cura di) (2021), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Università degli Studi di Torino, 2021
- A. CELOTTO (2020), *Algoritmi e algoretica: quali regole per l'intelligenza artificiale?*, in "Consulta online - Liber amicorum per Pasquale Costanzo", 27 marzo 2020
- S. CIVITARESE MATTEUCCI (2019), *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità*, in "Diritto pubblico", 2019, n. 1
- T. CORMEN, C. LEISERSON, R. RIVEST, C. STEIN (2010), *Introduzione agli algoritmi e strutture dati*, McGraw-Hill, 2010
- V. CORNELI (2023), *Sovranità tecnologica: intelligenza artificiale e valori costituzionali*, in "Forum di Quaderni Costituzionali", 2023, n. 2
- D. DALFINO (2020), *Decisione amministrativa robotica ed effetto performativo. Un beffardo algoritmo per una "buona scuola"*, in "Questione giustizia", 13 gennaio 2020
- P. DE HERT, S. GUTWIRTH (2009), *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action*, in S. Gutwirth, Y. Pouillet, P. De Hert et al., "Reinventing data protection", Springer, 2009
- A. DE LUCA (2018), *Big data analytics e data mining. Estrarre valore dai dati*, IPSOA, 2018
- G. DELLA MORTE (2018), *Big data e protezione internazionale dei diritti umani. Regole e conflitti*, Editoriale Scientifica, 2018
- M. DELMASTRO, A. NICITA (2019), *Big data. Come stanno cambiando il nostro mondo*, il Mulino, 2019
- P. DI CIOMMO (2023), *La prospettiva del controllo nell'era dell'Intelligenza Artificiale: alcune osservazioni sul modello Human In The Loop*, in "federalismi.it", 2023, n. 9
- EUROPEAN DATA PROTECTION BOARD (2020), *Guidelines 4/2019 on Article 25 –Data Protection by Design and by Default*, 2020
- D.G. FINK (1967), *Mente umana e cervelli elettronici. Introduzione all'intelligenza artificiale*, Zanichelli, 1967 (trad. it. A. Piccato, Mondadori, 2023)

- V. FROSINI (1968), *Cibernetica, diritto e società*, Edizioni di Comunità, 1968
- D.-U. GALETTA (2023), *Human-stupidity-in-the-loop? Riflessioni (di un giurista) sulle potenzialità e i rischi dell'Intelligenza Artificiale*, in "federalismi.it", 2023, n. 5
- D.-U. GALETTA, J.G. CORVALÁN (2019), *Intelligenza artificiale per una Pubblica amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in "federalismi.it", 2019, n. 3
- G. GALLONE (2023), *Riserva di umanità e funzioni amministrative*, Cedam Wolters Kluwer, 2023
- P. GHAVAMI (2019), *Data Analytics Methods*, De Gruyter, 2019
- E. GIORGINI (2019), *Algorithms and Law*, in "The Italian Law Journal", 2019, n. 1
- H.A. KISSINGER, E. SCHMIDT, D. HUTTENLOCHER (2023), *L'era dell'intelligenza artificiale. Il futuro dell'identità umana* (trad. it. A. Piccato), Mondadori, 2023
- A. LALLI (a cura di) (2024), *La regolazione pubblica delle tecnologie digitali e dell'intelligenza artificiale*, Giappichelli, 2024
- G. MALGIERI, G. COMANDÉ (2017), *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in "International Data Privacy Law", vol. 7, 2017, n. 4
- F.M. MANCIOPPI (2024), *La regolamentazione dell'intelligenza artificiale come opzione per la salvaguardia dei valori fondamentali dell'UE*, in "federalismi.it", 2024, n. 7
- B. MARCHETTI (2021), *La garanzia dello human in the loop alla prova della decisione amministrativa algoritmica*, in "BioLaw Journal - Rivista di BioDiritto", 2021, n. 2
- D. MARTIRE (2024), *Human in the loop. L'essere umano come fattore condizionante della – o condizionato dalla – intelligenza artificiale*, in "Rivista italiana di informatica e diritto", 2024, n. 2
- A. MASUCCI (1993), *L'atto amministrativo informatico. Primi lineamenti di una ricostruzione*, Jovene, 1993
- V. MAYER-SCHÖNBERGER, K. CUKIER (2013), *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Garzanti, 2013
- F. MIDIRI (2016), *La giuridificazione della protezione dei dati personali in Italia*, in "giustamm.it - Rivista di diritto pubblico", 2016, n. 5
- J.L. MONINO, S. SEDKAOUI (2016), *Big data, open data and data development*, Wiley, 2016
- C. NAPOLI (2020), *Algoritmi, intelligenza artificiale e formazione della volontà pubblica: la decisione amministrativa e quella giudiziaria*, in "Rivista AIC", 2020, n. 3
- M. NEGNEVITSKY (2002), *Artificial intelligence: a guide to intelligent systems*, Addison Wesley, 2002
- I.A. NICOTRA, V. VARONE (2019), *L'algoritmo, intelligente ma non troppo*, in "Rivista AIC", 2019, n. 4
- N.J. NILSSON (2002), *Intelligenza artificiale* (ed. it. a cura di S. Gaglio), Apogeo, 2002
- T. NUMERICO (2021), *Big data e algoritmi. Prospettive critiche*, Carocci, 2021
- A. PAJNO, F. DONATI, A. PERRUCCI (a cura di) (2022), *Intelligenza artificiale e diritto: una rivoluzione?*, il Mulino, 2022
- F. PATRONI GRIFFI (2018), *La decisione robotica e il giudice amministrativo*, in "giustizia-amministrativa.it", 28 agosto 2018 e confluito in A. Carleo (a cura di), "Decisione robotica", il Mulino, 2019
- J.S. PEDERSEN (2019), *Big data*, Edward Elgar, 2019
- W. PEDRYCZ, S.M. CHEN (2017), *Data Science and Big Data. An Environment of Computational Intelligence*, Springer, 2017

- L.R. PERFETTI (2017), Beyond the chinese room. Appunti per una riflessione su intelligenza artificiale e diritto pubblico, in "P.A. Persona e Amministrazione", 2017, n. 1
- F. PIZZETTI (2018), *Intelligenza artificiale, protezione dei dati e regolazione*, Giappichelli, 2018
- O. POLLICINO, M. BASSINI (2017), *Art. 8 Protezione dei dati di carattere personale*, in R. Mastroianni, O. Pollicino, S. Allegrezza et al. (a cura di) (2017), "Carta dei diritti fondamentali dell'Unione europea", Giuffrè, 2017
- C.S.R. PRABHU, A. SREEVALLABH CHIVUKULA, A. MOGADALA et al. (2019), *Big Data Analytics: Systems, Algorithms, Applications*, Springer, 2019
- G. RESTA (2019), *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in "Politica del diritto", 2019, n. 2
- R. REVLIN (2014), *Psicologia cognitiva. Teoria e pratica* (trad. it. M. Tartari), Zanichelli, 2014
- A. REZZANI (2013), *Big data. Architettura, tecnologie e metodi per l'utilizzo di grandi basi di dati*, Maggioli, 2013
- L. RINALDI (2022), Intelligenza artificiale, diritti e doveri nella Costituzione italiana, in "DPCE online", 2022, n. 1
- S. RODOTÀ (1973), *Elaboratori elettronici e controllo sociale*, il Mulino, 1973
- S. RUSSELL, P. NORVIG (2021), *Intelligenza artificiale: un approccio moderno* (ed. it. a cura di F. Amigoni), Pearson Prentice Hall, IV ed., 2021
- P. SEVERINO (a cura di) (2022), *Intelligenza artificiale. Politica, economia, diritto, tecnologia*, Luiss University Press, 2022
- A. SIMONCINI (2023), Il linguaggio dell'intelligenza artificiale e la tutela costituzionale dei diritti, in "Rivista AIC", 2023, n. 2
- A. SIMONCINI (2019), L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà, in "BioLaw Journal - Rivista di BioDiritto", 2019, n. 1
- A. SIMONCINI, S. SUWEIS (2019), *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in "Rivista di filosofia del diritto", 2019, n. 1
- M. SOMALVICO (1987), *Intelligenza artificiale*, Hewlett Packard, 1987
- E. STRADELLA (2019), La regolazione della Robotica e dell'Intelligenza artificiale: il dibattito, le proposte, le prospettive. Alcuni spunti di riflessione, in "MediaLaws. Rivista di Diritto dei Media", 2019, n. 1
- R. SUSSKIND (2019), *L'avvocato di domani. Il futuro della professione legale tra rivoluzione tecnologica e intelligenza artificiale* (trad. it. G. Bizzarri), Guerini Next, 2019
- P. TABOSSI (1988), *Intelligenza naturale e intelligenza artificiale. Introduzione alla scienza cognitiva*, il Mulino, 1988
- G. TIBERI (2007), *Riservatezza e protezione dei dati personali*, in M. Cartabia (a cura di), "I diritti in azione. Universalità e pluralismo dei diritti fondamentali nelle Corti europee", il Mulino, 2007
- A. TURING (1950), Computing machinery and intelligence, in "Mind", vol. 59, 1950, n. 236
- S. VACCARI (2019), *Note minime in tema di Intelligenza Artificiale e decisioni amministrative*, in "giustamm.it - Rivista di diritto pubblico", 2019, n. 10
- L. VAIANA (1996), *Il dizionario dell'intelligenza artificiale*, Istituto di Storia della filosofia, 1996
- L. VIOLA (2018), L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte, in "federalismi.it", 2018, n. 21
- N. WIENER (1948), *Cybernetics, or control and communication in the animal and the machine*, I ed., The MIT Press, 1948



ILDE FORGIONE

La prospettiva dell'intelligenza artificiale nel procedimento e nell'attività amministrativa

Il presente lavoro analizza l'impatto dell'utilizzo dei sistemi di intelligenza artificiale nell'esercizio delle funzioni pubbliche, con particolare attenzione alle conseguenze derivanti dalla delega di compiti complessi a tali strumenti, anche nell'ambito dei procedimenti discrezionali. In tale contesto, si riflette su come l'automazione decisionale possa influire sulla trasparenza, sul giusto procedimento e sulla responsabilità umana, elementi fondamentali per garantire la legittimità dell'azione amministrativa, nonché sul ruolo da attribuire all'AI. nel contributo verranno analizzate la normativa, nazionale ed europea in materia, nonché l'impostazione giurisprudenziale, che riflettono un'attenzione crescente verso la trasparenza e la responsabilità, aspetti considerati essenziali per l'adozione sicura ed efficace dell'AI nei contesti pubblici.

*Intelligenza artificiale – Pubblica amministrazione – AI governance – Discrezionalità
Ruolo degli algoritmi nel procedimento*

The perspective of artificial intelligence in administrative procedures and activities

The present work analyzes the impact of the use of artificial intelligence systems in the exercise of public functions, with particular attention to the consequences of delegating complex tasks to such tools, even in discretionary proceedings. In this context, it reflects on how decision automation may affect transparency, due process, and human responsibility – key elements for ensuring the legitimacy of administrative actions – as well as the role to be attributed to AI. The paper examines national and European legislation on the matter, as well as the jurisprudential approach in the field, which reflect a growing focus on transparency and accountability – considered essential aspects for the safe and effective adoption of AI in public contexts.

*Artificial intelligence – Public administration – AI governance – Administrative discretion
Role of algorithms in the procedure*

L'Autrice, PhD in Diritto pubblico e dell'economia, è dirigente presso il Ministero dell'Economia e delle Finanze. Le opinioni espresse nel presente contributo sono a titolo personale e non vincolano in alcun modo l'Amministrazione di appartenenza

Questo contributo fa parte della sezione monografica *Cittadini e pubbliche amministrazioni tra AI e diritto all'umano*, a cura di Enrico Carloni

SOMMARIO: 1. Introduzione: tra la macchina e l'umano. – 2. Il ricorso agli algoritmi come modello organizzativo. – 3. Le nuove garanzie a tutela dei privati nel procedimento algoritmico. – 4. Discrezionalità e intelligenza artificiale. – 5. Il *quantum* di contributo umano necessario. – 6. Conclusioni.

1. Introduzione: tra la macchina e l'umano

La domanda sottesa al presente lavoro è cosa accade quando l'esercizio dei compiti pubblici non è affidato unicamente ai funzionari amministrativi. La decisione di ricorrere (o meno) a una macchina per svolgere valutazioni complesse, impattanti su rilevanti interessi pubblici o privati, ove è essenziale che vi sia trasparenza delle motivazioni che hanno portato a un determinato risultato, deve confrontarsi con la necessità di mantenere le garanzie del giusto procedimento.

Posto che l'esercizio delle funzioni pubbliche può realizzarsi mediante il ricorso a sistemi di intelligenza artificiale (AI), la composizione degli interessi in gioco come sopra accennati va ricercata, da un lato, nella consapevolezza della non autosufficienza della decisione automatizzata e, dall'altro, nella corretta governance del fenomeno nonché nel principio di responsabilità umana.

Come è evidente, la riflessione sul procedimento amministrativo va declinata in ragione del coinvolgimento delle macchine aventi intelligenza e logica peculiari.

Sebbene le macchine siano estremamente efficienti nello sviluppare correlazioni complesse, risulta difficile ottenere una spiegazione o rilevare gli

errori computazionali¹. Invero, la predetta spiegazione, allorché riferita alla logica utilizzata dagli algoritmi di intelligenza artificiale, non assicura la piena comprensibilità della valutazione effettuata, per via dei non lineari collegamenti che sono in grado di sviluppare.

Posta l'opportunità del ricorso a tali strumenti nell'ambito dell'azione amministrativa, anche ai fini di miglioramento dell'efficienza e dell'efficacia², occorre chiedersi se il ricorso (legittimo) all'AI debba fondarsi su di una legislazione che le attribuisca tale specifica facoltà, ed a quali principi e regole si debba fare riferimento.

In ambito europeo, la prospettiva di una decisione sinergica tra le due intelligenze, umana e artificiale, è stata indagata a partire dal 2018 con la Strategia per la creazione di regole armonizzate per l'intelligenza artificiale³, fino ad arrivare al Regolamento UE 2024/1689, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale (c.d. AI Act). L'approccio in parola è volto a regolare i rischi legati all'implementazione e all'uso di alcune forme di AI, tenuto conto dell'importanza delle predette tecnologie per lo sviluppo economico dell'Unione e della necessità di rispettare i diritti fondamentali delle persone⁴.

1. LONGO 2022.

2. In questo senso le pronunce del Consiglio di Stato, 8 aprile 2019, n. 2270; 13 dicembre 2019, n. 8472; 4 febbraio 2020, n. 881.

3. *Communication on Artificial Intelligence for Europe*, SWD(2018) 137, seguita dal White paper on *Artificial Intelligence. A European approach to excellence and trust*, COM(2020) 65.

4. In particolare, nel considerando n. 1. L'approccio ricalca quello già proposto dal HIGH-LEVEL EXPERT GROUP ON AI 2019.

Nell'ordinamento nazionale, atteso che le tecnologie informatiche da «apparecchi di semplice registrazione di dati complessi, sono divenuti poi apparecchi di accertamento e verifica, di calcolo, di partecipazione a fasi procedurali di istruttoria, e infine di decisione», utilizzati «proprio per amministrare» proiettandosi sempre più verso l'esterno⁵, il legislatore è stato dapprima spinto a codificare i principi di legalità algoritmica⁶ con una norma settoriale ma di rilevanza sistemica (art. 30 d.lgs. 31 marzo 2023, n. 36, Codice dei contratti pubblici); quindi, è stato spinto a discutere in maniera compiuta dei principi che informano l'uso dell'intelligenza artificiale per settori specifici, inclusa la pubblica amministrazione⁷.

2. Il ricorso agli algoritmi come modello organizzativo

Nelle more dell'adozione della normativa primaria, occorre interrogarsi circa l'impatto degli strumenti tecnologici sull'esercizio del potere pubblico⁸.

Giacché il principio di legalità afferisce alla genesi e all'attribuzione del potere e non al modulo organizzativo del suo esercizio, l'automazione procedimentale non necessiterebbe di una norma primaria che ne espliciti la sua configurabilità ove costituisca un nuovo strumento radicalmente innovativo di estrinsecazione della prerogativa pubblica.

Diversamente, una copertura normativa diviene necessaria là dove l'impiego dell'intelligenza artificiale conduca alla costituzione di un nuovo potere⁹.

L'individuazione dell'opzione preferibile dipende da molteplici fattori.

Primariamente viene in rilievo il ruolo svolto dall'algoritmo nel procedimento, cioè, se esso sia un semplice strumento di supporto ovvero sia impiegato per prendere decisioni autonome, sostituendo il funzionario umano.

L'AI quando viene utilizzata per fornire informazioni o segnalazioni che vengono poste alla base della decisione umana – similmente a quanto avviene mediante il ricorso ad algoritmi basati su modelli e su regole rigide (*hard rules*) che seguono istruzioni chiare e definite, portando a risultati certi e predeterminati – può comunque essere inquadrata in termini di modello organizzativo, in quanto non sostituisce la decisione umana. Siamo dinanzi a una diversa modalità di esercizio del potere autoritativo, comunque già configurato e attribuito dall'ordinamento e di cui si conferma la competenza e responsabilità.

Per cui, l'istruttoria algoritmica, svolta tramite gli strumenti di AI, resta comunque sottoposta a regimi di controllo e motivazione, in grado di assicurare la compatibilità delle procedure e delle decisioni a valle con il patrimonio delle garanzie proprie del diritto amministrativo, sebbene vengano in rilievo regole, diverse e ulteriori da quelle individuate dalla legge n. 241/1990.

Nell'ordinamento interno un generale riferimento alla strumentalità della tecnologia all'azione amministrativa si rinviene nell'art. 3-*bis* della legge n. 241/1990. La disposizione, nello stabilire che le amministrazioni pubbliche agiscono mediante strumenti informatici e telematici per conseguire maggiore efficienza nella loro attività, implicitamente stabilisce l'estraneità del software all'attività amministrativa in senso stretto e la sua non riconducibilità al concetto di atto. Una ulteriore disposizione che dà conferma dell'algoritmo in termini di scelta organizzativa e di strumentalità della tecnologia all'azione amministrativa è l'art. 41 del Codice dell'amministrazione digitale (d.lgs. 7 marzo 2005, n. 82), secondo cui «le pubbliche amministrazioni gestiscono i procedimenti amministrativi utilizzando le tecnologie dell'informazione e della comunicazione».

5. Dal *Rapporto sui principali problemi dell'amministrazione dello Stato*, presentato nel 1979 dall'allora ministro della Funzione pubblica Massimo Severo Giannini.

6. CARLONI 2020.

7. Si tratta dell'Atto Senato n. 1146, recante Disposizioni e delega al Governo in materia di intelligenza artificiale, attualmente in esame nella 8ª Commissione.

8. Sul tema, in generale, si veda OTRANTO 2021.

9. Ha sottolineato l'esigenza di un fondamento normativo che consenta di ricondurre l'uso degli algoritmi nel perimetro del principio di legalità CIVITARESE MATTEUCCI 2019.

Infatti, come è stato sottolineato, l'algoritmo costituisce, nella sua dimensione statica, «l'oggetto della volizione amministrativa preliminare con cui si opta per l'automazione»¹⁰, ciò in quanto gli strumenti informatici non vengono formati all'interno del contesto procedimentale da un funzionario amministrativo¹¹. Si colloca, di conseguenza, nella fase preliminare relativa alla scelta di automatizzare il procedimento. Tale impostazione pare essere confermata dal disegno di legge sull'intelligenza artificiale¹² attualmente all'esame del Parlamento ove l'art. 13, rubricato *Uso dell'intelligenza artificiale nella pubblica amministrazione*, comma 2, prevede che «l'utilizzo dell'intelligenza artificiale avviene in funzione strumentale e di supporto all'attività provvedimentale».

Ma al di là della prospettiva *de iure condendo*, allo stato attuale possiamo affermare che l'uso dell'AI nel procedimento può discendere da una norma di rango primario – costituendo la base giuridica per l'applicazione a un numero indefinito di procedimenti di una certa categoria – ovvero da un regolamento¹³ o da un atto amministrativo a carattere generale, che costituisce la *lex specialis* di uno specifico procedimento come, ad esempio, un bando di gara¹⁴. Nel primo caso, si ha una disciplina legale che puntualizza le modalità di spendita del potere; nel secondo caso si ha un autovincolo amministrativo circa le modalità di esercizio del potere; in entrambe le ipotesi, vi sarebbe una determinazione preliminare attraverso cui si stabilisce di far ricorso all'automazione nello svolgimento dell'agire pubblico.

Inoltre, esaminando l'algoritmo e il software nella loro dimensione operativa, ci si accorge come essi, lungi dall'essere riconducibili agli atti amministrativi, abbiano piuttosto la natura di strumenti materiali al servizio del titolare dell'organo. Sul punto occorre distinguere ulteriormente l'ipotesi

in cui il software viene impiegato tra la fase istruttoria e quella decisionale ricevendo dati in input e, seguendo una sequenza di istruzioni predeterminata, genera un output, dall'ipotesi in cui l'AI viene utilizzata in fase decisoria.

Non desta particolari criticità l'uso degli algoritmi nella fase istruttoria, dal momento che l'automazione qui viene sicuramente a rappresentare una modalità operativa all'interno del procedimento amministrativo, un'attività materiale, priva di rilevanza giuridica esterna, finalizzata a supportare l'esercizio del potere e a realizzare le decisioni amministrative. Invero, benché l'automazione possa influire sulla fase istruttoria, essa non costituisce un'attività giuridica in senso stretto e neppure una decisione autonoma. Si rileva altresì che il risultato è espresso in linguaggio macchina, cioè un linguaggio non intellegibile dall'uomo senza un'apposita interfaccia¹⁵.

Questo approccio è stato recentemente accolto anche dalla giurisprudenza, la quale considera l'uso dell'algoritmo non come un atto giuridico, ma come modulo organizzativo, strumento procedurale e istruttorio all'interno del procedimento amministrativo soggetto alle verifiche tipiche dello stesso¹⁶.

Così argomentando, il risultato prodotto dall'algoritmo non rappresenta un provvedimento, ma una risultanza istruttoria (art. 6, co. 1, lett. e) della legge n. 241/1990) che necessita di un ulteriore atto di volontà da parte dell'amministrazione per tradursi in un provvedimento finale con efficacia esterna.

Pertanto, due momenti decisionali si distinguono nell'automazione: uno iniziale, in cui l'amministrazione sceglie di adottare l'algoritmo, e uno finale, in cui l'output viene recepito nel provvedimento conclusivo. In altri termini, l'algoritmo opera in funzione strumentale a un organo di cui

10. GALLONE 2023.

11. Sul ruolo dei tecnici informatici si veda PREVITI 2022.

12. Per il dossier ed approfondimenti sull'iter di approvazione si rimanda a Parlamento Italiano - *Disegno di legge S. 1146* - 19^a Legislatura.

13. Questo è l'approccio adottato, ad esempio, dalla Banca d'Italia, con il Regolamento 22 marzo 2022, n. 112.

14. L'uso dell'intelligenza artificiale nel settore dei contratti pubblici è stato compiutamente disciplinato dalla Parte II del Titolo I del d.lgs. n. 36/2023.

15. OROFINO 2002.

16. Da ultimo Cons. Stato, n. 8474/2019.

titolare rimane il funzionario preposto, esprimendo solo una «volontà potenziale»¹⁷ che dovrà essere fatta propria e manifestata nel provvedimento.

Nella differente ipotesi degli algoritmi di AI (in particolare, *deep learning*, etc.), capaci di apprendere autonomamente e di prendere decisioni senza l'intervento umano diretto, il rapporto tra le valutazioni svolte dalla macchina in sede istruttoria e quelle umane in sede decisoria diventa più complesso, sollevando questioni in punto di prevedibilità e trasparenza. Emerge la maggiore forza persuasiva del risultato fornito da uno strumento tecnologico, ritenuto generalmente più preciso e neutrale rispetto alle valutazioni svolte da un essere umano¹⁸.

Volendo ora analizzare l'intelligenza artificiale utilizzata in sede decisoria, occorre nuovamente distinguere la tipologia di algoritmo. Infatti, l'algoritmo *rule-based* non suscita perplessità in quanto i calcoli che esegue sono basati su una logica deterministica, secondo criteri stabiliti a monte dall'amministrazione, secondo il linguaggio di programmazione; di conseguenza, il processo decisionale, sebbene portato a termine dalla macchina, rimane indirettamente in capo alla p.a. che ha definito a monte i parametri di calcolo.

Nella diversa ipotesi in cui si faccia ricorso ad un algoritmo *machine learning*, la decisione si sposta dalla sfera umana (dell'amministrazione e del programmatore) alla macchina stessa, rendendo più difficile risolvere le problematiche legate alla legalità dell'algoritmo come questione organizzativa, dal momento che è assente qualsiasi intervento umano nel processo di elaborazione dei dati¹⁹. In tale ipotesi, infatti, è unicamente il software a determinare, anche formalmente, l'assetto degli interessi o dei rapporti, non essendo previsto l'intervento del funzionario persona fisica.

Seppure allo stato attuale il ricorso ad algoritmi aperti rimane confinato all'assistenza e supporto del decisore umano, che adotta la decisione, tuttavia, è innegabile che gradualmente tali sistemi verranno impiegati sempre più anche per l'*adjudication* e

la *regulation*²⁰. Di conseguenza, diventa tanto più rilevante la previsione di una necessaria "riserva di umanità", ovvero, di un intervento umano nel corso del procedimento, a monte o a valle di esso.

Nell'ambito dell'attività della pubblica amministrazione lo *human-in-the-loop*, oltre ad essere inevitabile sul piano giuridico, appare indispensabile per sfruttare caratteristiche peculiari dell'uomo, come la capacità di interpretare un contesto e prendere decisioni guidate da principi etici.

Come già accennato, una più compiuta sistemazione della materia ha trovato recentemente il suo fondamento nel regolamento europeo sull'intelligenza artificiale. Tale disciplina si applica anche ai soggetti pubblici utilizzatori di sistemi di AI, disegnando una cornice di regole incentrata sul grado di rischio dei citati sistemi.

Il principio etico-giuridico dello *human-in-the-loop* è ora sancito nell'articolo 14 dell'AI Act, rubricato *Human oversight*, il quale non riguarda però tutti i sistemi di AI, ma solo quelli ad alto rischio, così classificati nell'Allegato III. Inoltre, affinché i sistemi rimangano classificati come ad alto rischio, l'amministrazione dovrà svolgere una valutazione del rischio *in concreto* (art. 27 par. 1).

Il legislatore europeo vieta chiaramente l'uso dei sistemi di *deep learning* senza supporto umano per le attività classificate come ad alto rischio²¹. Tuttavia, per ragioni di generalità e astrattezza, non si rinviene una definizione dei citati sistemi, ma nel regolamento sono enucleati i criteri per individuarli (art. 6), nonché i settori di riferimento (Allegato III).

Di conseguenza, rimane da chiarire se il procedimento amministrativo sia da includere nelle attività ad alto rischio. La risposta rimane aperta e non può, ancora una volta, che essere valutata caso per caso a fronte di una verifica in concreto, sostanziale. Ciò può avvenire nell'ipotesi in cui esso ricada in uno dei settori individuati dalla normativa europea *a priori* come ad alto rischio – ed è il caso degli ambiti della *gestione e funzionamento delle infrastrutture critiche*, dell'*accesso*

17. GALLONE 2023.

18. LOGG-MINSON-MOORE 2019.

19. Considerando n. 67 e art. 13, par. 3, lett. vi) dell'AI Act.

20. COGLIANESE-LEHR 2019.

21. Art. 14, par. 1.

e fruizione di prestazioni e servizi pubblici o della gestione e funzionamento della fornitura di acqua, gas, riscaldamento, energia elettrica e infrastrutture digitali critiche – sia che si faccia riferimento alla presenza, alla luce della loro finalità prevista, di *un alto rischio di pregiudicare la salute e la sicurezza o i diritti fondamentali delle persone*²².

3. Le nuove garanzie a tutela dei privati nel procedimento algoritmico

Premessa dunque la generale ammissibilità degli strumenti di intelligenza artificiale nel procedimento, va rilevato che la loro introduzione si accompagna a una rinuncia essenziale dei diritti di partecipazione nel procedimento. Non sono infatti presenti i diritti sanciti a garanzia del privato dalla legge n. 241/1990 – ovvero quelli di partecipazione, di accesso, di pubblicità e di difesa – in ragione delle caratteristiche intrinseche delle decisioni algoritmiche, le quali non ammettono le forme classiche del contraddittorio e sono pure difficilmente spiegabili.

Poiché non è possibile rinunciare alle tutele proprie dello Stato di diritto nei confronti di una decisione autoritativa della p.a., occorre individuare dei nuovi limiti all'esercizio del potere tramite l'intelligenza artificiale e delle nuove garanzie a tutela del cittadino, al fine di rendere compatibili con l'ordinamento il ricorso a tali strumenti e sfruttarne gli effetti positivi in termini di efficienza ed efficacia.

In mancanza di un quadro normativo di riferimento, il Consiglio di Stato ha tentato una ricostruzione dell'assetto di tutele a partire dal Regolamento europeo sulla privacy e, nello specifico, mediante il ricorso agli artt. 13, 14, 15 e 22²³, dai quali si ricava il diritto dell'interessato ad essere informato dell'esistenza di un procedimento automatizzato nei suoi confronti, a ricevere informazioni precise sulla logica posta alla base del sistema e sulle conseguenze nei suoi confronti, nonché il divieto di decisioni esclusivamente automatizzate.

Vengono in rilievo, dunque, due elementi di garanzia minima, che costituiscono una sorta di evoluzione delle garanzie tradizionali e risultano più aderenti alla natura e alle caratteristiche delle decisioni algoritmiche. Emerge, da un lato, la piena conoscibilità del modulo utilizzato e dei criteri applicati, dall'altro, l'imputabilità della decisione, che deve restare in capo all'organo titolare del potere decisionale.

Sotto il primo profilo, la trasparenza²⁴ assume un'importanza cruciale anche con riferimento ai soggetti incisi dall'esercizio del potere. Il meccanismo attraverso cui si giunge alla decisione deve essere comprensibile e spiegabile; a tal fine, i diversi componenti dell'algoritmo devono essere garantiti «in tutti gli aspetti: dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti»²⁵. Ciò al fine di poter verificare che i criteri, i presupposti e gli esiti del procedimento robotizzato siano conformi alle prescrizioni e alle finalità stabilite dalla legge o dalla stessa amministrazione a monte di tale procedimento e affinché siano chiare – e conseguentemente sindacabili – le modalità e le regole in base alle quali esso è stato impostato²⁶. La necessità di predisporre «meccanismi in grado di decifrare la logica» degli algoritmi porta con sé, come conseguenza, che il principio di conoscibilità debba essere completato dal «principio di comprensibilità, ovvero sia la possibilità, per riprendere l'espressione del regolamento, di ricevere “informazioni significative sulla logica utilizzata”»²⁷.

Consapevole del pericolo che la *black box* si ponga come ostacolo a effettivi ed esaustivi accertamenti sulla correttezza delle singole fasi procedurali e sull'adeguatezza della motivazione posta alla base del provvedimento, l'AI Act intende la trasparenza come principio generale e impone alcuni obblighi informativi e requisiti di trasparenza minimi. Questi devono essere sufficienti a

22. Considerando 52.

23. Cfr. Cons. Stato, n. 881/2020.

24. Sulla trasparenza si rimanda a CARLONI 2022.

25. Sull'uso dei big data si v. COSTANTINO 2019 e, sia consentito, FORGIONE 2021.

26. Cons. Stato, n. 2270/2019.

27. Cons. Stato, n. 881/2020.

comprendere almeno le basi su cui si fonda l'iter logico seguito dal sistema, la cui intensità muta in relazione al livello di rischio dei sistemi²⁸. In particolare, l'articolo 13 prevede che i sistemi di intelligenza artificiale ad alto rischio sono progettati e sviluppati in modo tale da consentire agli utilizzatori di interpretare l'output e utilizzarlo adeguatamente.

Sotto il secondo profilo, deve essere assicurata l'imputabilità della decisione in capo a un funzionario umano (profilo della responsabilità), che deve essere in grado di verificarne logicità e legittimità. Ciò è essenziale per garantire che la decisione sia imputabile all'organo che detiene il potere, secondo il principio di legalità, e che sia possibile individuare chiaramente il soggetto responsabile²⁹. Tale verifica è posta a garanzia dell'amministrazione stessa, oltre che dei soggetti che sono influenzati dall'azione amministrativa gestita attraverso l'algoritmo.

A tal proposito, la normativa europea ha introdotto, oltre alle garanzie di trasparenza, prima con il Regolamento privacy (art. 22 par. 1), poi con il Regolamento sull'AI (art. 14), un limite esplicito all'uso di processi decisionali completamente automatizzati. Secondo quanto disposto dall'AI Act le misure di sorveglianza umane devono essere integrate nel sistema, fin dalla sua progettazione se tecnicamente possibile, ovvero almeno individuate dal fornitore in modo da poter essere successivamente attuate dal *deployer*. Inoltre, il legislatore europeo, consapevole dei rischi connessi all'*automation bias*, ha previsto che il sistema di AI deve consentire alle persone fisiche di rimanere consapevoli «della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'output», in particolare, per quei sistemi «utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche» (art. 14, par. 4, lett. b).

Nell'ordinamento nazionale le costanti riflessioni della letteratura scientifica e della giurisprudenza hanno condotto, come detto, alla positivizzazione dei canoni della legalità algoritmica con l'art. 30 del d.lgs. n. 36/2023. Proprio affinché la macchina non abbia un potere e dominio assoluto sui procedimenti il comma 3, lett. b) della menzionata disposizione ha sancito il principio di «non esclusività della decisione algoritmica», dal momento che il contributo umano deve poter avere l'ultima parola in merito alla correttezza o, meglio, in ordine alla legittimità della scelta, appunto controllando, validando o smentendo la decisione automatizzata.

Inoltre, la stessa giurisprudenza interna aveva già evidenziato che, «al fine di applicare le norme generali e tradizionali in tema di imputabilità e responsabilità, occorre garantire la riferibilità della decisione finale all'autorità ed all'organo competente in base alla legge attributiva del potere»³⁰.

In quest'ottica, anche in presenza di decisioni automatizzate, il principio di imputazione dell'atto e della relativa responsabilità deve essere coerente con il principio di immedesimazione organica, assicurando che l'autorità titolare del potere decisionale sia in grado di verificare la logicità e la correttezza degli esiti prodotti dall'algoritmo. Quest'ultimo, pur fungendo da strumento tecnico nella fase decisoria, non può sostituirsi completamente all'autorità competente, la quale deve valutarne gli esiti, ove decida di conformarsi ad essi, assumendo la responsabilità finale della decisione. In altri termini, l'algoritmo, e il software che ne è espressione in linguaggio macchina, non esprime «alcuna decisione, non sostanziandosi in una manifestazione di volontà»³¹.

Di conseguenza, il primo rilevante problema sarà quello di definire, nel rispetto di quanto preteso dall'art. 30, come debbano essere interpretate in concreto la «conoscibilità e comprensibilità» delle decisioni assunte mediante automazione. Si

28. Considerando n. 27.

29. GALLONE 2023.

30. Cons. Stato, n. 881/2020. La giurisprudenza amministrativa, tra l'altro, ha sottolineato l'importanza della Carta della Robotica (Risoluzione 2018/C 252/25) come punto di riferimento per affrontare le sfide poste dall'imputabilità e dalla responsabilità nelle decisioni automatizzate. La Carta, tra l'altro, sottolinea che, «nell'ipotesi in cui un robot possa prendere decisioni autonome, le norme tradizionali non sono sufficienti per attivare la responsabilità per i danni» da esso causati, poiché queste non permetterebbero di identificare chiaramente il soggetto autore della condotta illecita e conseguentemente esigere la riparazione della conseguenza dannosa.

31. GALLONE 2023.

fa riferimento specificamente alla traduzione in linguaggio giuridico della regola tecnica e del funzionamento dell'algoritmo, nonché dei criteri di valutazione. Emerge così il rischio che la proposta algoritmica venga validata solo formalmente dal funzionario che assume la decisione, in quanto privo delle competenze per metterne in discussione il risultato.

In secondo luogo, il sacrificio dei diritti di partecipazione varia in relazione alla tipologia di algoritmo, *rule-based* o *machine learning*, nonché al grado di discrezionalità del provvedimento finale. Infatti, in un procedimento standardizzato ed a basso contenuto discrezionale la compressione dei diritti di partecipazione può risultare poco impattante a fronte della relativa facilità nel ricostruire il percorso logico seguito dal software, sulla base degli input inseriti³². Diversamente, in un procedimento svolto con algoritmi di *machine learning* o *deep learning*, è dequotata la possibilità del privato di intervenire nel procedimento presentando memorie e documenti al fine di orientare la decisione ed approntare tutele riguardo ad *errori, guasti o incongruenze che possono verificarsi all'interno del sistema o nell'ambiente in cui esso opera, in particolare a causa della loro interazione con persone fisiche o altri sistemi* (art. 15.3 AI Act).

Difatti, con riferimento agli apporti partecipativi previsti dagli artt. 9 e 10 della l. n. 241/1990, l'inevitabile innalzamento del livello di tecnicità del procedimento non può spingersi al punto di depotenziare la concreta contestabilità della decisione da parte dell'interessato, «non soltanto sotto il profilo della sua conformità ai parametri legali, ma anche in relazione alla sua credibilità razionale»³³.

4. Discrezionalità e intelligenza artificiale

Con riferimento ai provvedimenti discrezionali, dal momento che non è possibile attribuire alla macchina una volontà propria, il ruolo dell'intelligenza artificiale potrà essere quello di ampliare gli strumenti conoscitivi e valutativi dell'amministrazione, rafforzandone la capacità orientativa.

Di conseguenza, il ruolo dell'intelligenza artificiale potrà declinarsi in un'attività di supporto al decisore pubblico nell'individuazione delle opzioni possibili, di definizione dei parametri da prendere in considerazione, di misurazione degli effetti e dell'impatto di una decisione e, in generale, di contributo al bilanciamento in concreto tra costi e benefici delle varie alternative in gioco, così da attribuire ad ognuna «un valore indicizzabile e confrontabile con altri»³⁴. L'AI viene cioè a collocarsi nell'ambito di un'operazione amministrativa³⁵ complessa, intesa come l'insieme di tutte le attività sistematicamente connesse, finalizzate alla risoluzione di un problema unitario che conduca a comporre un assetto di interessi.

In quest'ottica, viene rimodellata e riallocata anche la discrezionalità amministrativa, il cui spazio si sposterà più a monte, in sede di decisione di ricorrere all'intelligenza artificiale e nell'indicazione alla macchina dei parametri da seguire, nonché di una scala di priorità, similmente a quanto avviene con l'introduzione di autolimiti all'esercizio del potere, ovvero a valle, in sede di scelta della soluzione che massimizza l'interesse pubblico tra quelle proposte.

In altri termini, «la discrezionalità amministrativa, se senz'altro non può essere demandata al software, è quindi da rintracciarsi al momento dell'elaborazione dello strumento digitale»³⁶, ovvero nel momento in cui si seleziona l'opzione maggiormente adeguata agli scopi perseguiti dall'amministrazione. Ciò consente di rilevare una certa predeterminazione della decisione.

Inoltre, in mancanza di una differente indicazione normativa, l'amministrazione è libera di scegliere se ricorrere o meno all'AI nell'attività procedimentale, cioè può autonomamente valutare quale sia il percorso migliore per realizzare il fine pubblico. Ne discende che tale scelta attiene al merito amministrativo, ossia allo spazio di opportunità che permane all'interno della discrezionalità e che non è sindacabile in sede giurisdizionale. Il giudice potrà contestare il risultato dell'elaborazione del

32. MARCHETTI 2022.

33. SIMEOLI 2022.

34. CASSATELLA 2021.

35. D'ORSOGNA 2005.

36. Cons. Stato, n. 2270/2019.

software o il suo funzionamento, ma non la scelta di ricorrere all'automazione.

Indubbiamente, l'AI può garantire risultati soddisfacenti nell'acquisizione di un contesto informativo³⁷ il più possibile esteso, di fondamentale importanza per la formazione di un volere amministrativo maggiormente consapevole. La decisione costituisce non già una qualsiasi soluzione del problema bensì quella più conveniente e che, nella vicenda concreta, maggiormente soddisfa l'interesse pubblico. Si può apprezzare l'uso dell'intelligenza artificiale come supporto non soltanto nell'ambito del procedimento amministrativo, ma anche per le scelte organizzative dell'amministrazione o nella gestione del rischio, ad esempio nel campo dell'ordine pubblico e della sicurezza³⁸.

In una simile prospettiva, spetta all'autorità amministrativa la decisione di indirizzo delle attività, determinando gli scopi da raggiungere e delineando il contesto in cui ci si muove. L'intelligenza artificiale, in ottica servente, sarebbe quindi a supporto della valutazione in ordine alla praticabilità o desiderabilità delle opzioni precedentemente formulate, anche in rapporto agli obiettivi perseguiti. Per cui, la discrezionalità verrebbe attratta nell'ambito dell'istruttoria e orientata alla costruzione razionale della questione di fatto, nonché alla verifica della necessità di cura in concreto dell'interesse pubblico.

In capo all'amministrazione è posto poi il generale dovere di motivare e giustificare la decisione³⁹, indicando le ragioni che hanno condotto a quella specifica composizione di interessi sia con riferimento alla ragionevolezza-proporzionalità dell'alternativa selezionata rispetto alle finalità dell'azione amministrativa e all'impatto sulle prerogative delle altre parti coinvolte. Per tale via, l'organo titolare della decisione si assumerebbe la responsabilità dell'output fornito dal software e dei

suoi impatti. Questi, una volta individuate le conseguenze derivanti dall'attuazione della soluzione prospettata, sarebbe chiamato ad argomentare circa la compatibilità e la coerenza della rappresentazione con le finalità perseguite nella decisione di indirizzo⁴⁰.

Di talché, è posto in capo all'amministrazione l'onere di assunzione di responsabilità con riferimento alla scelta delle misure informatiche più adatte a gestire l'istruttoria con salvezza dei diritti procedurali, ma non anche con riferimento alla scelta di ricorrere all'uso delle macchine per gestire il procedimento.

L'intelligenza artificiale potrebbe infine produrre anche un positivo impatto sulla trasparenza, dal momento che la definizione delle alternative a disposizione del decisore pubblico avviene all'esito «dell'applicazione di una metodologia prestabilita, attraverso cui si è impostato ed affrontato il problema, e non di scelte rimesse all'intuito o alle capacità dei singoli funzionari ed organi»⁴¹.

5. Il *quantum* di contributo umano necessario

In ultimo, si pone la questione relativa al *quantum* di contributo umano necessario per elevare l'output del software a decisione legittima ovvero per smentire, eventualmente, il risultato della macchina. Anche qui la risposta non può essere univoca, poiché il problema si deve porre e raffrontare con riferimento alle specifiche tipologie di procedimento e al loro concreto sviluppo.

Il funzionario umano non può svolgere solo un ruolo marginale di fronte all'imperante presenza della macchina, ma deve avere una sua centralità, tale per cui possa confrontarsi con l'intelligenza artificiale senza subirla. Vi è il rischio che sia difficile contestare il risultato della macchina tenuto conto della sua forza persuasiva e dell'alleggerimento

37. PAOLANTONIO 2021.

38. Per una rassegna sull'uso dell'AI a supporto di decisioni discrezionali si veda ancora CASSATELLA 2021. Sull'impatto degli algoritmi nell'organizzazione amministrativa si v. anche AUBY 2019.

39. Oltre alla legge sul procedimento amministrativo, la giurisprudenza ha fatto riferimento dell'art. 42 (*Right to a good administration*) della Carta Europea dei Diritti Fondamentali, a cui fa riferimento anche il considerando n. 48 del Regolamento AI.

40. CASSATELLA 2021. In tal senso, cfr. anche le già menzionate sentenze del Consiglio di Stato.

41. CASSATELLA 2021.

dal peso della decisione e della sua motivazione per il funzionario⁴². In aggiunta, detto rischio è aggravato dai limiti insiti nel funzionario, come il pregiudizio cognitivo o i c.d. *bias* di conferma, e dai pregiudizi sociali che inevitabilmente entrano a far parte dell'algoritmo, tramite i dataset di *training*⁴³. In quest'ottica diventa rilevante la formazione: il non subire l'intelligenza artificiale passa attraverso un funzionario che ne conosce il funzionamento ed è consapevole delle insidie che si celano dietro la tecnologia⁴⁴.

Se dal punto di vista teorico la soluzione appare piuttosto semplice, restano ancora molte criticità relative all'esercizio concreto del potere che potranno essere sciolte, anche solo a livello operativo, mediante il massivo ricorso all'AI nell'azione dell'amministrazione.

La compatibilità della decisione algoritmica con i principi dell'ordinamento non può che essere perseguita mediante un sistema di training dell'algoritmo adeguato al tipo di attività, nonché, in particolar modo, con la predisposizione di meccanismi che permettano di controllare, verificare, validare, rigettare la decisione algoritmica, o anche interrompere il funzionamento della macchina là dove ciò sia necessario per evitare effetti pregiudizievoli.

L'esigenza di un controllo umano non viene declinata dal legislatore (europeo e nazionale)

nella definizione di requisiti specifici e ben perimetrati quanto, piuttosto, in una rosa di possibilità di intervento sull'elaborato finale della macchina. Tali possibilità ben potranno essere sviluppate in pratiche operative puntuali per ogni settore di attività⁴⁵ e dovranno al contempo essere supportate a monte da un'adeguata formazione del personale, affinché sia in grado di comprendere la logica ed il funzionamento dei sistemi, così come richiesto dalla normativa europea (art. 4 del Regolamento sull'AI)⁴⁶.

6. Conclusioni

Sebbene l'opzione prudentiale, guidata dal principio di precauzione⁴⁷, al momento sembra essere ancora la migliore da seguire con riferimento all'uso ed al ruolo dell'intelligenza artificiale nel procedimento e nell'attività amministrativa, rispetto al recente passato, è innegabile che la definizione di un quadro normativo più puntuale, unita alla elaborazione di alcuni principi da parte della giurisprudenza, abbia condotto a una maggiore un'apertura degli spazi di trasparenza. A ciò si aggiunge la spinta verso la formazione e consapevolezza dei titolari degli organi decisorii che potrebbe risolvere alcune delle criticità emerse con riferimento al ruolo di questi strumenti.

Anzi, l'entrata in vigore del regolamento 2024/1689 ha chiarito che gli algoritmi di

42. Sui rischi legati ai fenomeni di *self-prophecy*, che potrebbero replicare i medesimi errori che il ricorso alla tecnologia mira ad evitare si veda LETTIERI 2021.

43. GALETTA 2023, ha coniato l'espressione di "human stupidity in the loop" con riferimento al rischio che «l'Intelligenza Artificiale, invece di potenziare l'intelligenza umana, funga da effetto moltiplicatore delle imperfezioni della stessa».

44. CHITI-MARCHETTI-RANGONE 2022, a cui si rimanda anche per un'analisi casistica dei vari utilizzi dell'AI da parte dei soggetti pubblici.

45. Il considerando 93 attribuisce un ruolo fondamentale ai *deployer* di sistemi di AI in quanto essi «sono nella posizione migliore per comprendere come il sistema di IA ad alto rischio sarà utilizzato concretamente e possono pertanto individuare potenziali rischi significativi non previsti nella fase di sviluppo, in ragione di una conoscenza più puntuale del contesto di utilizzo e delle persone o dei gruppi di persone che potrebbero essere interessati, compresi i gruppi vulnerabili».

46. L'art. 30 co 3 lett. b) del d.lgs. n. 36/2023 richiede che comunque esista «nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatizzata». Similmente, il Regolamento AI, all'art. 14, par. 4 riconosce agli operatori la possibilità di: d) decidere, in qualsiasi situazione particolare, di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l'output del sistema; e) intervenire sul funzionamento o interrompere il sistema mediante un pulsante di "arresto" o una procedura analoga.

47. A cui ha fatto riferimento il Parlamento europeo nel 2017 con la citata Risoluzione C 252/254.

intelligenza artificiale ad alto rischio non possono mai essere intesi come sostituti integrali degli organi titolari del potere decisionale ed ha posto alcune condizioni a garanzia dell'intervento umano nel procedimento automatizzato.

Sinteticamente, dall'analisi svolta si possono ricavare alcune conclusioni relative allo svolgimento dell'attività amministrativa tramite gli strumenti di AI, tenendo bene a mente che il processo di *juridification* non si è esaurito ed è destinato a evolvere ancora nel futuro.

Innanzitutto, la tecnologia è servente alla valutazione umana, come di recente confermato anche dal legislatore italiano nel disegno di legge sull'intelligenza artificiale. La decisione di ricorrere a tali strumenti è rimessa infatti all'apprezzamento dell'autorità e la definizione delle caratteristiche dello specifico software è riservata alla stessa, supportata dai programmatori.

In secondo luogo, più che nella definizione di specifici requisiti per il ricorso a tali strumenti, il legislatore (europeo e nazionale) e la giurisprudenza hanno formalizzato alcuni principi e garanzie – a tutela dei soggetti coinvolti nel procedimento e in funzione di *accountability* dell'amministrazione – che vanno a sostituire la perdita delle prerogative

di partecipazione previste dalla legge, in quanto non praticabili nel mutato contesto digitale.

In terzo luogo, uno spazio applicativo per l'intelligenza artificiale nell'ambito della discrezionalità amministrativa può essere ricavato nella realizzazione di una più funzionale ed efficiente organizzazione dei servizi, nonché, per supportare il decisore nella generazione di scenari – anche di lungo periodo e in grado di evidenziare costi e benefici – a valle delle singole opzioni.

In conclusione, l'ingresso degli strumenti di intelligenza artificiale nel contesto pubblico può costituire l'occasione non soltanto di renderlo più efficiente ed efficace in base ai classici schemi di azione, quanto di ripensare e innovare i modi di svolgimento dell'attività amministrativa, integrando tra loro norma, procedimento e strumenti di gestione della conoscenza, tra cui in particolare i sistemi informatici, in una logica funzionale a migliorare la qualità dell'azione amministrativa, sia per i destinatari sia per gli attori della stessa. Per fare ciò e creare valore pubblico aggiunto, occorre dunque eleggere i contesti in cui lo sviluppo dei sistemi di intelligenza artificiale massimizza marginalmente la performance del lavoro umano (ad esempio, audit, frodi, programmazione e progettazione).

Riferimenti bibliografici

- J.-B. AUBY (2019), *Il diritto amministrativo di fronte alle sfide digitali*, in "Istituzioni del Federalismo", 2019, n. 3
- E. CARLONI (2022), *Il paradigma trasparenza. Amministrazioni, informazione, democrazia*, il Mulino, 2022
- E. CARLONI (2020), *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in "Diritto Amministrativo", 2020, n. 2
- A. CASSATELLA (2021), *La discrezionalità amministrativa nell'età digitale*, in Aa.Vv., "Scritti per Franco Gaetano Scoca", vol. I, Edizioni Scientifiche Italiane, 2021
- E. CHITI, B. MARCHETTI, N. RANGONE (2022), *L'impiego di sistemi di intelligenza artificiale nelle pubbliche amministrazioni italiane: prove generali*, in "BioLaw Journal - Rivista di BioDiritto", 2022, n. 2
- S. CIVITARESE MATTEUCCI (2019), *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità*, in "Diritto pubblico", 2019, n. 1
- C. COGLIANESE, D. LEHR (2019), *Transparency and Algorithmic Governance*, in "Administrative Law Review", vol. 71, 2019, n. 1
- D. D'ORSOGNA (2005), *Contributo allo studio dell'operazione amministrativa*, Editoriale Scientifica, 2005
- I. FORGIONE (2021), *L'esercizio del potere tramite i dati, tra logica small e big data*, in Gruppo di Pisa, "Dibattito aperto sul Diritto e la Giustizia Costituzionale", Quaderno n. 3, 2021

- D.-U. GALETTA (2023), *Human-stupidity-in-the-loop? Riflessioni (di un giurista) sulle potenzialità e i rischi dell'Intelligenza Artificiale*, in "federalismi.it", 2023, n. 5
- G. GALLONE (2023), *Riserva di umanità e funzioni amministrative*, CEDAM, 2023
- HIGH-LEVEL EXPERT GROUP ON AI (2019), *Ethics Guidelines for Trustworthy AI*, Bruxelles, 2019
- N. LETTIERI (2021), *Contro la previsione. Tre argomenti per una critica del calcolo predittivo e del suo uso in ambito giuridico*, in "Ars interpretandi", 2021, n. 1
- J.M. LOGG, J.A. MINSON, A. MOORE (2019), *Algorithm appreciation: People prefer algorithmic to human judgment*, in "Organizational Behavior and Human Decision Processes", vol. 151, 2019
- E. LONGO (2022), *I processi decisionali automatizzati e il diritto alla spiegazione*, in A. Pajno, D. Donati, A. Perrucci (a cura di), "Intelligenza artificiale e diritto: una rivoluzione?", vol. I, il Mulino, 2022
- B. MARCHETTI (2022), voce *Amministrazione digitale*, in "Enciclopedia giuridica", Treccani, 2022
- A.G. OROFINO (2002), *La patologia dell'atto amministrativo elettronico: sindacato giurisdizionale e strumenti di tutela*, in "Foro Amministrativo - CdS", 2002
- P. OTRANTO (2021), *Riflessioni in tema di decisione amministrativa, intelligenza artificiale e legalità*, in "federalismi.it", 2021, n. 7
- N. PAOLANTONIO (2021), *Il potere discrezionale della pubblica automazione. Sconcerto e stilemi (sul controllo giudiziario delle "decisioni algoritmiche")*, in "Diritto amministrativo", 2021, n. 4
- L. PREVITI (2022), *La decisione amministrativa robotica*, Editoriale Scientifica, 2022
- D. SIMEOLI (2022), *L'automazione dell'azione amministrativa nel sistema delle tutele di diritto pubblico*, in A. Pajno, D. Donati, A. Perrucci (a cura di), "Intelligenza artificiale e diritto: una rivoluzione?", vol. I, il Mulino, 2022



BENEDETTO PONTI

Il fornitore dell'algoritmo quale soggetto estraneo all'amministrazione

L'outsourcing costituisce una soluzione consolidata per l'organizzazione e le prestazioni di servizi pubblici (e in certi casi anche di funzioni pubbliche in senso stretto). Lo è anche con riferimento ai processi di digitalizzazione di infrastrutture, servizi strumentali, risorse di calcolo funzionali all'esercizio di funzioni pubbliche. Sotto questo profilo, la questione del *fornitore dell'algoritmo* in quanto *extraneus* (sotto il profilo soggettivo) rispetto all'amministrazione costituisce un tema per certi versi consueto. Il contributo muove da un quesito: quando l'oggetto dell'outsourcing è un prodotto o una soluzione basata sull'intelligenza artificiale, le categorie interpretative tradizionali mantengono la loro utilità, oppure l'outsourcing dell'intelligenza artificiale modifica i termini del discorso? L'analisi mostra come, nonostante alcune categorie interpretative mantengano la loro validità, l'importazione dell'AI nel contesto dei poteri pubblici presenti tratti peculiari, che derivano dalla struttura di mercato in cui l'AI viene sperimentata, prodotta e commercializzata, così come da alcune specifiche caratteristiche funzionali "di fondo", diremmo implicite, e che come tali meritano di essere poste in evidenza. Queste sottolineature offrono anche una chiave di lettura per leggere la fornitura dei servizi basati su AI dalla prospettiva del GDPR e da quella del regolamento sull'intelligenza artificiale.

Outsourcing – Amministrazione pubblica – Intelligenza artificiale – Asimmetria – Neoliberismo

Outsourcing artificial intelligence in public administration

For the planning and execution of public services (and occasionally even public functions in the strict sense), outsourcing is an established approach. This also holds true for the processes of digitizing infrastructure, auxiliary services, and computing resources that are functional or otherwise used to support the performance of public duties. In this regard, the issue of the algorithm's provider acting as an extraneus (in a subjective sense) to the administration is a recurring one. The concern presented at the starting point of the study is whether standard interpretative categories remain relevant when the goal of outsourcing is an artificial intelligence-based product or solution, or does artificial intelligence outsourcing alter the discourse's terms? The analysis shows how, despite the validity of some interpretive categories, the AI importing in the context of public powers presents unique characteristics that stem from the market structure in which AI is produced, marketed, and tested as well as from certain implicit, functional, characteristics. As such, these characteristics should be emphasized. Specific issues that occur in the operation of outsourcing artificial intelligence services in the context of public authorities can be verified using the AI Act and the GDPR.

Outsourcing – Public administration – Artificial intelligence – Asymmetry – Neoliberalism

L'Autore è professore associato di Diritto amministrativo presso l'Università degli studi di Perugia

Questo contributo fa parte della sezione monografica *Cittadini e pubbliche amministrazioni tra AI e diritto all'umano*, a cura di Enrico Carloni

SOMMARIO: 1. L'intelligenza artificiale tra Stato e big tech. – 2. L'AI come caso specifico di IT outsourcing. – 3. Il potere di agenda del fornitore esterno. – 4. Ci sono caratteri intrinseci dell'intelligenza artificiale? – Il funzionario pubblico di fronte all'AI.

1. L'intelligenza artificiale tra Stato e big tech

Questo contributo intende riflettere sulla configurazione dell'intelligenza artificiale (AI, con specifico riferimento a quella specifica tecnologia basata sul *machine/deep learning*) quale soluzione o strumento da applicare (in modo più o meno diretto) all'esercizio delle funzioni pubbliche. Intende farlo, muovendo da una constatazione, ovvero che questa tecnologia è attualmente sviluppata, prodotta e commercializzata al di fuori del settore pubblico, e che pertanto la messa al servizio dell'AI a scopi "pubblicistici", comporta che essa sia oggetto di fornitura dall'esterno. Su questa circostanza di fatto paiono esserci pochi dubbi, e le ragioni che hanno condotto a questa constatazione sono molteplici.

Sebbene l'indagine non abbia ad oggetto la ricostruzione di queste ragioni, converrà fare cenno a due di esse, che non solo appaio tra loro consequenziali, ma che hanno anche un notevole impatto sull'economia complessiva delle riflessioni che intendiamo proporre.

In primo luogo, occorre tenere a mente che l'outsourcing costituisce una soluzione organizzativa che risponde all'impostazione neoliberista del rapporto tra Stato e mercato. Secondo questa dottrina¹ spetta al mercato (perché più efficiente) sviluppare e produrre innovazione, da mettere poi (eventualmente) al servizio delle funzioni che spettano ai poteri pubblici esercitare. La dottrina neoliberale dello *Stato minimo*, infatti, non contempla un'autonoma capacità dei poteri o dei soggetti

pubblici di mantenere, promuovere e sviluppare linee produttive in capo al settore pubblico. Entro questa cornice concettuale, dunque, gli *strumenti* di cui i poteri pubblici si servono per il disbrigo dei propri compiti, sono *naturaliter* attinti e/o ritratti dal mercato, secondo schemi anche differenziati tra loro (in ragione dell'intensità con la quale il fornitore *extraneus* – di mercato – di una soluzione di carattere strumentale è coinvolto nella organizzazione del relativo servizio), ma che possono essere accomunati e qualificati nei termini dell'*outsourcing*². Questa nozione appare preferibile, a tali fini, rispetto a quella corrispondente di *esternalizzazione*, dal momento che questa seconda pare presupporre un movimento dall'interno verso l'esterno, ossia un contesto organizzativo in cui le attività (i servizi, le soluzioni organizzative) che pertengono (in modo più o meno stabilizzato) al settore pubblico sono traslate all'esterno di questo: un contesto, dunque, che presuppone un perimetro del settore pubblico ancora ampio, e che comprende anche attività di produzione diretta di servizi strumentali. In effetti, le *esternalizzazioni* hanno rappresentato uno dei meccanismi mediante i quali il neoliberismo si è imposto anche con riferimento al ruolo e ai confini del settore pubblico, e rimandano quindi ad un'età di transizione, nel corso della quale detto perimetro si è andato progressivamente restringendo (anche per effetto, appunto, delle esternalizzazioni). La nozione di *outsourcing* appare preferibile, dunque, perché designa la modalità *ordinaria* (e, quasi, necessaria) per il settore pubblico di rifornirsi (*to source*)

1. BIRCH 2017; PECK 2010.

2. MARCO-SIMÓ-PASTOR-COLLADO 2020.

e organizzare gli strumenti (tecnologici, ma non solo), sviluppati, prodotti e commercializzati stabilmente al di fuori (*out*) dei propri confini.

Il secondo dato di contesto che preme segnalare è che lo sviluppo delle tecnologie e dei servizi di intelligenza artificiale è realizzato all'interno di un sistema industriale dominato da grandi soggetti privati (le cd. Big Tech, o GAFAM, etc.), e richiede una enorme quantità di risorse, non solo, economiche, ma anche fisiche e naturali³. Una circostanza, questa seconda, che è in (larga) parte un prodotto della prima, ma che contribuisce anche a consolidarne i contorni, dal momento che – nel contesto attuale – i poteri pubblici non potrebbero nemmeno “competere” con il settore privato, al fine di sviluppare e produrre *in house* tale tecnologia. Con la conseguenza che, con riferimento all'impiego dell'AI al servizio delle funzioni pubbliche, il ricorso all'outsourcing non costituisce un'opzione, ma una soluzione effettivamente necessitata, tenuto conto del contesto⁴.

2. L'AI come caso specifico di IT outsourcing

L'outsourcing costituisce una soluzione consolidata per l'organizzazione e la prestazione di servizi pubblici anche con riferimento ai processi di digitalizzazione di infrastrutture, servizi strumentali, risorse di calcolo funzionali (o comunque posti al servizio) dell'esercizio di funzioni pubbliche⁵. Sotto questo profilo, pertanto, porre a tema la questione del *fornitore dell'algoritmo* in quanto *extraneus* (sotto il profilo soggettivo) rispetto all'amministrazione costituisce una tematica per certi versi (già) tradizionale. E in effetti in letteratura sono significativi i tentativi di trarre indicazioni dall'esperienza dell'outsourcing pubblico nel settore delle

Information Technologies proprio con riferimento a quella specifica tecnologia identificata (in modo ancora molto ampio) in termini di Intelligenza artificiale⁶. Più in generale, si può affermare che secondo la letteratura prevalente⁷ il ricorso all'IA a supporto dell'esercizio di funzioni pubbliche, sembra presentare vantaggi e rischi che sono in buona parte riconducibili – in termini di tassonomia – a quelli già evidenziati, a suo tempo, con riferimento ai processi di digitalizzazione/automazione⁸.

Sul primo fronte, dominano i vantaggi (attesi) in termini di riduzione dei costi, di guadagni in termini di produttività, come pure quelli connessi ad una più sistematica capacità di analisi, così da prevenire o correggere errori, frodi, corruzione e più in generali fenomeni di *malpractice* connessi a spazi di discrezionalità non adeguatamente presidiati. Ma analoghi sono anche i vantaggi attesi in termini di *predisposizione* delle policy: già con riferimento alle precedenti stagioni della informatizzazione, le accresciute capacità conoscitive e di analisi conseguibili mediante lo sfruttamento delle basi di dati erano indicate quali fattori destinati a incidere in modo significativo sulle funzioni di programmazione delle politiche pubbliche. Oggi, tali vantaggi sono ascritti alle inedite modalità di analisi abilitate dall'applicazione di tecniche di *deep learning*, a cominciare ad esempio dai progetti connessi alla c.d. *smart cities*.

Anche sul fronte dei rischi (paventati), non è difficile scorgere alcuni specifici parallelismi e analogie. Ad esempio, è stato posto a tema il grado di calcolabilità (e automazione) del processo decisionale (o anche solo istruttorio), e il rischio di perdita di un grado desiderabile di discrezionalità *soggettiva* nell'esercizio di certe specifiche funzioni. Ancora, il tema della *qualità dei dati di input*

3. CRAWFORD 2021.

4. Infatti, anche qualora disponibile, l'alternativa rappresentata dal software o soluzioni di produzione pubblica o comunque “interna” al sistema pubblico è stata sempre più spiazzata (e rimpiazzata), per effetto di una serie di fattori concomitanti, e tra loro connessi: il progressivo impoverimento delle risorse (umane, oltre che finanziarie) necessarie a tali fini; la presunta neutralità tecnologica delle soluzioni prodotte dal mercato; la preferenza per il ricorso al mercato (perché più efficiente), il tutto entro un paradigma di *Stato minimo* che domina anche con riferimento alle tecnologie digitali (TORCHIA 2023).

5. GANTMAN 2011; MARCO-SIMÓ-PASTOR-COLLADO 2020; POUTVAARA-JORDAHL 2020.

6. DICKINSON-YATES 2023; COLLINGTON 2022.

7. COGLIANESE-LAI 2022; SUN-MEDAGLIA 2019; WIRTZ-WEYERER-GEYER 2019.

8. BERTOLUCCI 2024; OECD 2024.

precede, e di molto, la stagione dell'intelligenza artificiale applicata. Analogo è il tema dell'asimmetria informativa (nel rapporto coi fornitori privati) e quello (connesso) della perdita (o carenza strutturale) di un'adeguata *expertise* all'interno del perimetro pubblico. Analoghi sono, infine, i rischi paventati in termini di effetto netto di sostituzione della forza di lavoro umana.

Alla luce di queste (rilevanti) analogie, ciò che vorremmo evidenziare, dunque, sono quelle che ci appaiono essere le peculiarità (e gli specifici problemi) che caratterizzano quella specifica ipotesi/sottoinsieme/caso, ossia l'impiego dell'AI, entro un più generale contesto di outsourcing degli strumenti e delle infrastrutture di digitalizzazione da parte del settore pubblico.

3. Il potere di agenda del fornitore esterno

In primo luogo, la stessa nozione di outsourcing nel caso dell'intelligenza artificiale andrebbe precisata e contestualizzata, dal momento che il *fornitore esterno* non è solo quel soggetto dal quale l'amministrazione acquista (o acquisisce altrimenti il diritto all'uso di) un determinato software/soluzione *già completo e pronto per essere applicato* (salvo residuali adattamenti/customizzazioni). Va certamente inquadrata entro la prospettiva dell'outsourcing anche l'ipotesi in cui l'amministrazione cooperi "attivamente" alla progettazione della soluzione, insieme e accanto al fornitore, tutte le volte in cui il gap di *expertise* tra i due attori risulti così rilevante da configurare comunque il ruolo del fornitore ben al di là della soglia della mera *strumentalità*, e spesso anche oltre quello della partnership *paritaria* (o dialettica). Detto in altri termini, l'asimmetria informativa (e non solo informativa) che caratterizza questo genere di relazioni è tale da configurare in ogni caso un tasso di "autonomia" decisionale (in termini operativi, come pure di *agency*) in capo al fornitore, anche quando la soluzione (infine) adottata è destinata a operare ben all'interno dei confini soggettivi del soggetto pubblico erogatore del servizio (o titolare della funzione)⁹. Per le ragioni già evidenziate in

apertura, tale specifica situazione non costituisce un'eccezione, bensì la regola (o, quantomeno, la normalità), di talché appare del tutto implausibile immaginare che, nell'implementazione delle soluzioni di intelligenza artificiale propriamente detta, i pubblici poteri (e le pubbliche amministrazioni in particolare) siano configurabili (nel tempo concreto, attuale) come attori pienamente autonomi rispetto ai fornitori; l'intelligenza artificiale non rappresenta, pertanto, uno *strumento pienamente disponibile* agli attori pubblici, i quali sono quindi in qualche modo destinati a subire (in modo più o meno intenso, ma non evitabile) l'*agenda* dei produttori che forniscono loro tali servizi¹⁰.

In secondo luogo (come già sottolineato), il fornitore di IA è strutturalmente un soggetto estraneo all'amministrazione, dal momento che lo sviluppo ed il "dominio" di questa tecnologia appare saldamente di pertinenza di attori (che definirei *imprenditoriali* appare oramai riduttivo) che operano anche in relazione con i pubblici poteri e con le amministrazioni (a diversi livelli) ma che si collocano al di fuori (e ben distanti, sotto il profilo concettuale e deontico) dal relativo perimetro, soggettivo o oggettivo che questo sia.

La combinazione di questi due fattori (l'IA è un "prodotto", una "soluzione", un sistema di organizzazione e sfruttamento della conoscenza che viene fornito all'amministrazione da un soggetto ad essa estraneo, e che è in condizione di influenzarne l'agenda) giustifica quindi l'ipotesi di lavoro: verificare se l'AI abbia specifici caratteri, e quali questi siano, può infatti fornire indicazioni sull'effetto derivante dal suo impiego nell'ambito dell'esercizio delle funzioni pubbliche.

4. Ci sono caratteri intrinseci dell'intelligenza artificiale?

I rischi intrinseci connessi alla tecnologia dell'AI, con specifico riferimento a quelle tecniche di *deep learning* capaci di estrarre ed evidenziare correlazioni, ed utilizzate anche al fine di formulare specifiche inferenze (*predictive AI*), sono noti, e molto dibattuti¹¹. Tra i più dibattuti, vi sono quelli connessi all'*inevitabile* effetto di discriminazione che

9. KUZIEWSKI-MISURACA 2020.

10. Per una lettura radicale di questa asimmetria, tale per cui l'AI può essere controllata solo a mezzo di AI, cfr. HEIDELBERG 2024A; HEIDELBERG 2024B.

11. O'NEIL 2017; CHALLEN-DENNY-PIT et al. 2019.

deriva dalla circostanza che il *deep learning* opera un raggruppamento della popolazione sulla base di correlazioni che – appunto – trascurano questa o quella caratteristica statisticamente marginale (all'interno del gruppo, in ragione del criterio di correlazione operato), con effetti discriminatori più e più volte segnalati. Alcuni ritengono questa una caratteristica *di default*, e quindi ineliminabile/irrimediabile¹²; altri, invece, ritengono che questi limiti possono essere gestiti, sia in termini di mitigazione dei rischi, sia mediante lo sviluppo di un'etica dell'intelligenza artificiale¹³. In particolare, questo secondo approccio assume l'AI come uno strumento neutro (o neutralizzabile, con gli opportuni accorgimenti), e che su questa base esso può essere posto al servizio (in termini di razionalità strumentale) di questa o quella *mission*. Si muove su questa falsariga la recentissima regolamentazione dell'AI elaborata e approvata dall'Unione europea. Infatti, la classificazione delle soluzioni sulla base del rischio comporta che – laddove il livello di rischio non sia ritenuto inaccettabile – esso possa essere *mitigato* o comunque gestito mediante l'applicazione di una serie di meccanismi ed istituti (in particolare: requisiti specifici e obblighi in capo a fornitori e utilizzatori, i c.d. *deployer*)¹⁴.

Per economia di discorso, assumiamo che i rimedi proposti (ad esempio, quelli introdotti dall'*AI Act* dell'Ue) per mitigare e gestire i rischi connessi all'AI siano efficaci, senza per altro ignorare le critiche che sono state mosse in proposito (o, più in generale, in riferimento all'approccio regolatorio così adottato)¹⁵. Ciò perché vorremmo attirare l'attenzione su alcuni elementi caratteristici dell'AI che appaiono ulteriori (o, anche, collaterali) rispetto a quelli presi in considerazione dalla regolamentazione europea, e che pertanto prescindono dalla gestione del rischio così come *ivi* prefigurata

(ovvero, che vengono incisi solo marginalmente da tali rimedi).

In primo luogo, i sistemi di intelligenza artificiale si nutrono di dati, una mole immensa e sempre in aggiornamento. Adottare una soluzione di AI per l'esercizio di funzioni pubbliche non è quindi una soluzione neutra sotto il profilo del modello di business, dal momento che condiziona l'esercizio della funzione alla persistenza di tale sistema (che, anzi, così facendo, contribuisce a stabilizzare), che si fonda sulla produzione, l'accumulazione e il "consumo" dei dati. Ma non è neutra anche sotto un ulteriore, connesso profilo. Infatti, come sottolineato autorevolmente in letteratura¹⁶, il modello di business delle big tech è basato sul *surveillance advertising*, al punto che l'AI è stata definita «a derivative of surveillance»¹⁷. Ciò che è rilevante sotto una molteplicità di aspetti. Da una parte, infatti, l'adozione di soluzioni basate sull'AI comporta anche l'importazione di questo specifico approccio, in quanto in qualche modo connaturato al suo sviluppo e alle sue applicazioni. In secondo luogo, l'adozione di soluzioni basate sull'AI da parte del settore pubblico può, piuttosto, essere letta come l'immissione di questo secondo nel più complessivo *business model* costruito e alimentato dalle big tech, un ulteriore momento del processo di travaso di potere in favore di queste ultime («shift the matrix of social power»)¹⁸.

Sotto altro (ma connesso) profilo, i sistemi di intelligenza artificiale supportano la supremazia della razionalità strumentale, che è propria e costitutiva della logica politica del *neoliberismo*¹⁹. L'importazione di tale logica nell'ambito del settore pubblico non è affatto neutra, dal momento che rischia di incidere in modo significativo su altre, differenti logiche che possono (legittimamente) caratterizzare tanto la formulazione delle policy pubbliche, quanto (in certi contesti) anche

12. TAFANI 2023.

13. AGARWAL-BEYGEZIMER-DUDÍK et al. 2018; HACKER 2018.

14. WÖRSDÖRFER 2024; SCHUETT 2023; NOVELLI-CASOLARI-ROTOLO et al. 2023.

15. TAFANI 2023; LAUX-WACHTER-MITTELSTADT 2024.

16. ZUBOFF 2019.

17. WHITTAKER 2022.

18. DENCİK 2022.

19. MOROZOV 2023; MOROZOV 2019; BIRCH 2020.

lo loro concreta attuazione²⁰. Basti considerare – per riprendere il parallelo con le politiche di digitalizzazione – gli effetti prodotti anche su sistemi caratterizzati da una forte impronta solidaristica. Paradigmatico è, ad esempio, il caso della Danimarca, un paese scandinavo con un cospicuo *welfare state*, a lungo capace di guidare e sostenere il processo di digitalizzazione (le politiche di *egovernment*) secondo il paradigma che potremmo definire dell'*in-house providing*. Tuttavia, con l'ulteriore progressione ed approfondimento dei processi di digitalizzazione (dal 2005 in avanti) il sistema amministrativo danese ha conosciuto un doppio *retrenchment*: quello del *welfare state*, e quello della capacità di progettare, realizzare e gestire *in-house* le iniziative che richiedono una forte *expertise* nel campo delle IT²¹. Queste dinamiche sono tra loro strettamente interrelate. L'impatto di queste politiche sulla natura del *welfare state* (che acquista le sembianze di un *welfare surveillance state*) è stato già messo in evidenza²², insieme alla riconfigurazione dei caratteri della stessa cittadinanza, in quanto cittadinanza digitale, in senso pienamente neoliberista²³.

Va anche notato che in alcune esperienze più mature di *public in-house IT retrenchment*, il tentativo più recente di recuperare margini di capacità progettuale e di expertise da parte del settore pubblico ha prodotto risultati limitati (è il caso dell'UK)²⁴, a testimonianza di un assetto (la predominanza del fornitore privato di servizi IT) che va assumendo caratteri strutturali; caratteri che – con riferimento al sub-settore dell'AI – appaiono consolidati.

Infine, occorre tenere conto di due ulteriori aspetti, che caratterizzano in modo specifico i modi di produzione e riproduzione della conoscenza basati sull'intelligenza artificiale. In primo luogo, il calcolo basato sulla datizzazione di molteplici caratteristiche personali, catturate da dispositivi sempre più pervasivi, nel momento in cui viene applicato a fini predittivi e/o classificatori, finisce per *negare* la dimensione della libertà in quanto capacità di autodeterminazione da parte del singolo, che è invece preso in considerazione come essere statico, riconducibile a questa o quella categoria di appartenenza e trattato (in termini predittivi o regolatori) di conseguenza²⁵. Si tratta di una caratteristica intrinseca della logica dell'AI, che appare collidere con la concezione della persona umana in quanto agente dotato *per definizione* di autodeterminazione, e quindi, sempre per definizione, costitutivamente “non prevedibile”²⁶. Occorre quindi chiedersi se e come sia possibile “depurare” di questo aspetto (che appare determinante) l'AI, al fine di renderla compatibile con il suo impiego nell'ambito dell'esercizio delle funzioni pubbliche. Infine, si deve tenere conto della circostanza – variamente segnalata in letteratura – per la quale i sistemi di intelligenza artificiale tendono a risultare *conservative*, nella misura in cui (essendo alimentati ed allenati sulla base di dati raccolti *nel tempo passato*) tendono a riproporre, riprodurre (e anche, quindi, a consolidare) la realtà così come essa è (o è stata) rappresentata, registrata, colta in quelle informazioni²⁷. L'adozione dei sistemi di AI comporta dunque, in diversa misura (ma irrimediabilmente), la scelta di replicare il passato, occultando e legittimando (dietro la parvenza

20. WANG 2022; ALSHALLAQI 2024.

21. COLLINGTON 2022.

22. JØRGENSEN 2021; HJELHOLT 2024.

23. SCHOU-HJELHOLT 2019; SCHOU-HJELHOLT 2018; HINTZ-DENCIK-WAHL-JØRGENSEN 2018.

24. KATTEL-TAKALA 2021.

25. MATSUMI-SOLOVE 2023.

26. «Claiming to be able to predict human behaviour as precisely as one can predict that the milk in the fridge will go bad is tantamount to treating people as things. It denies the distinction between persons and things, i.e. between one who has rights, and is therefore a subject of the legal system, and one on which rights are exercised, and is therefore an object. This feature of treating people as things is a constitutive characteristic of predictive optimisation systems: the political qualities of such systems are therefore inherent and cannot be altered by any technical design choice» (TAFANI 2024, p. 10).

27. O'NEIL 2017; NUMERICO 2021; ZAJKO 2021.

dell'automazione) ineguaglianza, discriminazioni, squilibri di potere²⁸. Una caratteristica che appare incompatibile (quantomeno) con le potenzialità trasformative ed emancipatorie di un certo modo di intendere il ruolo dei poteri pubblici, nel contesto degli ordinamenti democratici, quelli cioè impegnati nella riduzione delle disuguaglianze e nella effettiva garanzia dei diritti fondamentali.

5. Il funzionario pubblico di fronte all'AI

Un'altra AI è possibile? Forse astrattamente è possibile immaginarla, ma l'AI *reale* oggi è pensata, sviluppata e realizzata secondo uno specifico approccio, che incorpora *by default* certi criteri di pre-comprensione e organizzazione della realtà, piuttosto che altri. In assenza di un'*expertise* "pubblica" da contrapporre a quella privata, l'introduzione di soluzioni di AI nel perimetro pubblico comporta inevitabilmente la necessità di addestrare i funzionari umani ad interloquire in modo appropriato, consoni, efficaci, con tali sistemi. Con la conseguenza che con il termine funzionario esperto, qualificato, *skillato*, si finirà per fare riferimento a quella classe di funzionari che – avendo appreso a interagire in modo coerente e consistente con questi sistemi – avranno assorbito (volenti o nolenti) le relative pre-impostazioni. Voglio dire: più il funzionario viene addestrato (con successo) ad interloquire efficacemente con questo genere di macchine, più esso si allontana dal (modello del) funzionario coerente (invece) con le esigenze del *diritto alla buona amministrazione*²⁹. Si tratterà di un funzionario *meno imparziale* (perché attratto nella specifica, parziale *weltanschauung* insita nell'AI così come effettivamente praticata); un funzionario sempre meno in grado di *rendere conto*³⁰, fornire motivazioni/giustificazioni diverse dalla *razionalità strumentale* così come identificata e controllata dall'AI, anche laddove gli spazi di discrezionalità potrebbero giustificare strategie di azione fondate su presupposti di razionalità e/o ragionevolezza anche differenti dalla sola razionalità strumentale; e questo, anche a prescindere

dalle difficoltà connesse alla *opacità intrinseca* dei sistemi di AI basati sul *deep learning*.

Per apprezzare l'impatto del framework che abbiamo tratteggiato, si prenda il caso delle soluzioni di AI che trattano dati personali. Come previsto dal GDPR, il trattamento dei dati personali da parte di una amministrazione pubblica è legittimato se e nella misura in cui esso risulta *necessario* «per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento»³¹. Ma chi progetta, sviluppa, allena e mette in cantiere i sistemi di AI non è l'amministrazione pubblica (titolare del trattamento), ma piuttosto il fornitore esterno, con tutte le conseguenze del caso, a cominciare dalla capacità di *traslare* nel settore pubblico le precomprensioni, le logiche e i caratteri che sono stati tratteggiati nei paragrafi precedenti. Anche al netto della mitigazione dei rischi (vedi alla voce *AI Act*), resta il fatto che l'AI è messa in opera all'interno di un rapporto fortemente asimmetrico, nell'ambito del quale la capacità *a monte* della parte pubblica di incidere in modo effettivo al fine di plasmare la soluzione o il sistema è estremamente ridotta. Ciò significa (anche) che lo spazio di legittimazione del trattamento, costituito dalla relazione di necessità che intercorre tra la modalità di trattamento di cui sono oggetto i dati personali, e il perseguimento degli interessi pubblici, è effettivamente "riempito" innanzitutto e soprattutto dal fornitore della soluzione di AI, il che comporta che il sistema di trattamento sarà condizionato dalle scelte, esplicite, implicite e latenti, effettuate dal fornitore; rispetto a queste scelte, l'amministrazione-titolare del trattamento non è in condizione di intervenire, sia per mancanza di adeguata *expertise*, sia in ragione dei vincoli legali che proteggono le privative industriali e la proprietà intellettuale del fornitore, sia perché nella maggior parte dei casi non è affatto consapevole della esistenza e della rilevanza di tali spazi di scelta. Questo esempio è anche utile per verificare quale ruolo possa essere giocato, *a valle*, dal funzionario pubblico, secondo l'approccio *human-in-the-loop*. Nella misura in cui le condizioni per un effettivo intervento in

28. MCQUILLAN 2023; VESA-TIERNARI 2023; PADDEN 2022.

29. GALETTA 2005.

30. CRAWFORD-SCHULTZ 2019.

31. PONTI 2023.

funzione di verifica e correzione risultano impegnative³², il funzionario rischia di operare (al più) come fattore di *legittimazione* di un meccanismo decisionale su cui non ha un effettivo controllo³³.

Riferimenti bibliografici

- A. AGARWAL, A. BEYGEZIMER, M. DUDÍK et al. (2018), *A reductions approach to fair classification*, in "Proceedings of the 35th International Conference on Machine Learning", vol. 80, 2018
- M. ALSHALLAQI (2024), *The complexities of digitization and street-level discretion: a socio-materiality perspective*, in "Public Management Review", vol. 26, 2024, n. 1
- M. BERTOLUCCI (2024), *L'intelligence artificielle dans le secteur public*, in "Revue de la littérature et programme de recherche. Gestion et management public", 2024, n. 5
- K. BIRCH (2020), Automated neoliberalism? The digital organisation of markets in technoscientific capitalism, in "New Formations", 2020, n. 100-101
- K. BIRCH (2017), *A Research Agenda for Neoliberalism*, Edward Elgar, 2017
- R. CHALLEN, J. DENNY, M. PITT et al. (2019), *Artificial intelligence, bias and clinical safety*, in "BMJ Quality & Safety", vol. 28, 2019, n. 3
- C. COGLIANESE, A. LAI (2022), *Algorithm vs. Algorithm*, in "Duke Law Journal", vol. 72, 2022
- R. COLLINGTON (2022), *Disrupting the Welfare State? Digitalisation and the Retrenchment of Public Sector Capacity*, in "New Political Economy", vol. 27, 2022, n. 2
- J. CONSTANTINO (2022), *Exploring Article 14 of the EU AI proposal: accountability challenges of the human in the loop when supervising high-risk AI systems in public administration*, 17 August 2022
- K. CRAWFORD (2021), *The atlas of AI: Power, politics, and the planetary costs of artificial intelligence*, Yale University Press, 2021
- K. CRAWFORD, J. SCHULTZ (2019), *AI Systems As State Actors*, in "Columbia Law Review", vol. 119, 2019, n. 7
- L. DENCİK (2022), *The Datafied Welfare State: A Perspective from the UK*, in A. Hepp, J. Jarke, L. Kramp, (eds), "New Perspectives in Critical Data Studies. Transforming Communications - Studies in Cross-Media Research", Palgrave Macmillan, 2022
- H. DICKINSON, S. YATES (2023), *From external provision to technological outsourcing: lessons for public sector automation from the outsourcing literature*, in "Public Management Review", vol. 25, 2023, n. 2
- D.-U. GALETTA (2005), *Il diritto ad una buona amministrazione europea come fonte di essenziali garanzie procedurali nei confronti della pubblica amministrazione*, in "Rivista italiana di diritto pubblico comunitario", 2005, n. 3-4
- S. GANTMAN (2011), *IT Outsourcing in the Public Sector: A Literature Analysis*, in "Journal of Global Information Technology Management", vol. 14, 2011, n. 2
- B. GREEN (2022), *The flaws of policies requiring human oversight of government algorithms*, in "Computer Law & Security Review", vol. 45, 2022
- P. HACKER (2018), *Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under eu law*, in "Common Market Law Review", vol. 55, 2018, n. 4

32. CONSTANTINO 2022.

33. GREEN 2022; PARASURAMAN-MANZEY 2022.

- R.L. HEIDELBERG (2024A), *Artificial Intelligence and the Modern Condition of Expertise*, in "Administration & Society", vol. 56, 2024, n. 1
- R.L. HEIDELBERG (2024B), *What's old is new: AI and bureaucracy*, in "Handbook on Public Policy and Artificial Intelligence", Edward Elgar Publishing, 2024
- A. HINTZ, L. DENCİK, K. WAHL-JØRGENSEN (2018), *Digital citizenship in a datafied society*, John Wiley & Sons, 2018
- M.F. HJELHOLT (2024), *The absorbent digital welfare state: Silencing dissent, steering progress*, in "Journal of Sociology", 22 May 2024
- R.F. JØRGENSEN (2021), *Data and rights in the digital welfare state: the case of Denmark*, in "Information, Communication & Society", vol. 26, 2021, n. 1
- R. KATTEL, V. TAKALA (2021), *Dynamic capabilities in the public sector: The case of the UK's Government Digital Service*, UCL Institute for Innovation and Public Purpose, Working Paper Series (IIPP WP 2021/01)
- M. KUZIEMSKI, G. MISURACA (2020), *AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings*, in "Telecommunications policy", vol. 44, 2020, n. 6
- J. LAUX, S. WACHTER, B. MITTELSTADT (2024), *Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk*, in "Regulation & Governance", vol. 18, 2024, n. 1
- J.M. MARCO-SIMÓ, J.A. PASTOR-COLLADO (2020), *IT Outsourcing in the Public Sector: A Descriptive Framework from a Literature Review*, in "Journal of Global Information Technology Management", vol. 23, 2020, n. 1
- H. MATSUMI, D.J. SOLOVE (2023), *The Prediction Society: AI and the Problems of Forecasting the Future*, GWU Legal Studies Research Paper No. 2023-58
- D. MCQUILLAN (2022), *Resisting AI: an anti-fascist approach to artificial intelligence*, Policy Press, 2022
- E. MOROZOV (2023), *The True Threat of Artificial Intelligence*, in "International New York Times", 30 June 2023
- E. MOROZOV (2019), *Capitalism's new clothes*, in "The Baffler", 4 February 2019
- C. NOVELLI, F. CASOLARI, A. ROTOLO et al. (2023), *Taking AI risks seriously: a new assessment model for the AI Act*, In "AI & Soc", 2023
- T. NUMERICO (2021), *Big data e algoritmi: Prospettive critiche*, Carocci, 2021
- C. O'NEIL (2017), *Weapons of math destruction: How big data increases inequality and threatens democracy*, Crown, 2017
- OECD (2024), *Governing with Artificial Intelligence: Are governments ready?*, OECD Artificial Intelligence Papers n. 20, OECD Publishing, 2024
- M. PADDEN (2023), *The transformation of surveillance in the digitalisation discourse of the OECD: a brief genealogy*, in "Internet Policy Review", vol. 12, 2023, n. 3
- R. PARASURAMAN, D.H., MANZEY (2010), *Complacency and Bias in Human Use of Automation: An Attentional Integration*, in "Human Factors: The Journal of the Human Factors and Ergonomics Society", vol. 52, 2010, n. 3
- J. PECK (2010), *Constructions of Neoliberal Reason*, Oxford University Press, 2010
- B. PONTI, (2023), *Attività amministrativa e trattamento dei dati personali: gli standard di legalità tra tutela e funzionalità*, FrancoAngeli, 2023

- P. POUTVAARA, H. JORDAHL (2020), *Public sector outsourcing*, in "IZA World of Labor", 2020, n. 65
- J. SCHOU, M. HJELHOLT (2019), *Digitalizing the welfare state: citizenship discourses in Danish digitalization strategies from 2002 to 2015*, in "Critical Policy Studies", vol. 13, 2019, n. 1
- J. SCHOU, M. HJELHOLT (2018), *Digital citizenship and neoliberalization: governing digital citizens in Denmark*, in "Citizenship Studies", vol. 22, 2018, n. 5
- J. SCHUETT (2023), *Risk Management in the Artificial Intelligence Act*, in "European Journal of Risk Regulation", 2023
- T.Q. SUN, R. MEDAGLIA (2019), *Mapping the challenges of Artificial Intelligence in the public sector: Evidence from public healthcare*, in "Government Information Quarterly", vol. 36, 2019, n. 2
- D. TAFANI (2024), *Do AI systems have politics? Predictive optimisation as a move away from the rule of law, liberalism and democracy*, in "Bollettino telematico di filosofia politica", 2024
- D. TAFANI (2023), *Predictive optimisation systems do not work, and they infringe rights. So why do we use them?*, in "Journal of Law, Market & Innovation", vol. 2, 2023, n. 3
- L. TORCHIA (2023), *Lo Stato digitale*, il Mulino, 2023
- M. VESA, J. TIENARI (2022), *Artificial intelligence and rationalized unaccountability. Ideology of the elites?*, in "Organization", vol. 29, 2022, n. 6
- G. WANG, S. XIE, X. LI (2024), *Artificial intelligence, types of decisions, and street-level bureaucrats: evidence from a survey experiment*, in "Public Management Review", vol. 26, 2024, n. 1
- M. WHITTAKER (2022), *A Message from Signal's New President*, September 6, 2022
- B.W. WIRTZ, J.C. WEYERER, C. GEYER (2019), *Artificial Intelligence and the Public Sector - Applications and Challenges*, in "International Journal of Public Administration", vol. 42, 2019, n. 7
- M. WÖRSDÖRFER (2024), *Mitigating the adverse effects of ai with the European Union's artificial intelligence act: Hype or hope?*, in "Global Business and Organizational Excellence", vol. 43, 2024
- M. ZAJKO (2021), *Conservative AI and social inequality: conceptualizing alternatives to bias through social theory*, in "AI & SOCIETY", vol. 36, 2021, n. 3
- S. ZUBOFF (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2019



MATTEO FALCONE

La *data science* come nuovo sapere per governare le intelligenze artificiali nelle pubbliche amministrazioni

In un contesto in forte trasformazione, dovuto alla crescita della complessità amministrativa, all'egemonia computazionale dei poteri privati e alla crescente legislazione, europea e nazionale, sui dati e sui sistemi di intelligenza artificiale (IA), è necessario che le amministrazioni comincino ad utilizzare le tecnologie algoritmiche per l'esercizio delle funzioni amministrative in modo consapevole. Partendo da queste premesse, l'autore riflette su quali saperi devono essere presenti nelle amministrazioni pubbliche per governare l'uso dei sistemi di IA per la cura degli interessi collettivi, evidenziando limiti e criticità della situazione attuale.

Competenze digitali – Data science – Amministrazione digitale – Intelligenza artificiale – Algoritmi

Data science as new knowledge for governing artificial intelligence in public administrations

In a rapidly changing context, due to the growth of administrative complexity, the computational hegemony of private powers and the growing European and national legislation on data and artificial intelligence systems, it is necessary for administrations to start using algorithmic technologies for the exercise of administrative functions in a conscious manner. Starting from these premises, the author reflects on what knowledge must be present in public administrations in order to govern the use of AI systems for the care of collective interests, highlighting limits and criticalities of the current situation.

Digital skills – Data science – Digital administration – Artificial intelligence – Algorithms

L'Autore è assegnista di ricerca in Diritto amministrativo e docente affidatario del corso di Diritto dell'informazione e della comunicazione presso l'Università di Perugia

Questo contributo fa parte della sezione monografica *Cittadini e pubbliche amministrazioni tra AI e diritto all'umano*, a cura di Enrico Carloni

SOMMARIO: 1. La trasformazione digitale pubblica tra complessità amministrativa ed egemonia computazionale dei poteri privati. – 2. La necessità di trasformare “digitalmente” le professionalità nelle amministrazioni pubbliche. – 2.1. *Le indicazioni normative sulle competenze digitali dei funzionari.* – 2.2. *Le politiche sulla diffusione delle competenze digitali nel sistema amministrativo.* – 3. L’esigenza di essere più coraggiosi: la necessità di una riflessione organica su competenze, professionalità e organizzazione del digitale. – 4. Una prospettiva alternativa: la *data science* come nuovo sapere per governare le intelligenze artificiali. – 5. La *data science* come sapere al servizio delle amministrazioni pubbliche.

1. La trasformazione digitale pubblica tra complessità amministrativa ed egemonia computazionale dei poteri privati

Nonostante l’informatizzazione e la digitalizzazione pubblica siano da decenni uno degli obiettivi prioritari degli indirizzi normativi e politico-amministrativi europei e nazionali¹, solo negli ultimi anni il sistema amministrativo italiano sembra andare verso una complessiva e più sostenuta trasformazione digitale.

Il Piano Nazionale di Ripresa e Resilienza (da ora PNRR), in modo particolare, ha accelerato notevolmente questa trasformazione, finanziando alcune politiche considerate centrali per garantire

servizi digitali pubblici integrati, interoperabili e sicuri. Basti pensare, ad esempio, alle politiche di migrazione dei dati e degli applicativi di molte amministrazioni verso servizi di *cloud computing* certificati (compreso il Polo Strategico nazionale), in particolare di quelle territoriali²; oppure alle politiche atte ad incrementare il livello di interoperabilità del sistema amministrativo attraverso la costruzione di specifici ecosistemi digitali³, utilizzando le *Application Programming Interface* (da ora API), che permettono l’accesso a piattaforme nazionali, come la Piattaforma Digitale Nazionale Dati (da ora PDND) e le basi di dati di interesse nazionale⁴; o ancora la predisposizione di interventi (e finanziamenti) per rafforzare la connettività del Paese, in particolare l’infrastruttura per

1. Per una ricostruzione delle politiche europee e nazionali sulla digitalizzazione pubblica che hanno interessato l’Italia negli ultimi decenni si v. CAIO 2014; Commissione parlamentare di inchiesta sul livello di digitalizzazione e innovazione delle Pubbliche Amministrazioni e sugli investimenti complessivi riguardanti il settore delle tecnologie e della comunicazione, *Relazione sull’attività svolta*, Roma, 26 ottobre 2017; Corte dei conti, *Referto in materia di informatica pubblica*, Roma, 26 novembre 2019. Anche nella riflessione amministrativistica sono emerse ricostruzioni storico-normative della vicenda. Per tutti si v. CIVITARESE MATTEUCCI-TORCHIA 2016, p. 155 ss.; CARLONI 2019; CAVALLO PERIN 2020; PIRAS 2020; MARCHETTI 2022.

2. Sulle strategie cloud computing per le amministrazioni e sul Polo Strategico nazionale nel PNRR si v. MONTAGNANI 2022.

3. Un esempio concreto della tendenza ordinamentale a costruire settorialmente ecosistemi digitali è l’ecosistema di approvvigionamento digitale, previsto dal d.lgs. 31 marzo 2023, n. 36. Per un approfondimento si v. CARULLO 2023; CAVALLO PERIN-LIPARI-RACCA 2024.

4. Cfr. CONTALDO 2022; ALBERTI 2022; SANDULLI 2021.

la fornitura delle connessioni veloci in tutto il territorio nazionale⁵.

Anche le linee di indirizzo del *Piano triennale per l'informatica nelle pubbliche amministrazioni 2024-2026* rappresentano plasticamente questa tendenza. Il nuovo documento definisce meglio metodi e contenuti di questo percorso di transizione, ricalibrando l'approccio degli ultimi anni, poco attento alla cura degli aspetti organizzativi e al complessivo coinvolgimento di tutto il sistema amministrativo nella trasformazione digitale. Basta leggere le prime pagine del Piano per rendersene conto: «le problematiche dell'amministrazione pubblica possono trovare nuove soluzioni grazie alla trasformazione digitale», ma solo «se questa viene vista come "riforma" dell'azione amministrativa e quindi come un nuovo tipo di "capacità istituzionale" che ogni ente pubblico deve strutturare nel proprio funzionamento interno ("riorganizzazione strutturale e gestionale" ex art. 15 CAD) ed esterno (facendo sistema con gli altri enti pubblici e anche con le imprese, i professionisti, le università/centri di ricerca, il terzo settore, ecc.)»⁶.

L'accelerazione della trasformazione digitale pubblica – a maggior ragione se intesa come un nuovo tipo di "capacità istituzionale" interna ed esterna, richiamando le parole del Piano – si inserisce, però, in un contesto sempre più complesso e particolarmente problematico. Una complessità dovuta principalmente a due fattori⁷.

Il primo fattore è la storica frammentazione informativa e tecnologica del sistema amministrativo italiano. Questo elemento è riconducibile, da un lato, all'autonomia organizzativa

delle amministrazioni, all'interno della quale rientrano tradizionalmente le scelte relative alla fornitura delle tecnologie informatiche e alla gestione dei dati in possesso delle amministrazioni. Dall'altro lato, al modo in cui si è costruita la digitalizzazione pubblica in Italia, sviluppatasi in modo pionieristico, episodico e senza un coordinamento nazionale, generando un contesto in cui ogni singola amministrazione aveva regole e tecnologie diverse⁸. Non per nulla tutte le politiche di digitalizzazione che si sono susseguite negli anni hanno provato a migliorare la circolazione delle informazioni per l'esercizio delle funzioni amministrative – in particolare di quelle "repubblicane", cioè che necessitano il coinvolgimento di più livelli di governo – e ad assicurare l'integrazione dei linguaggi degli strumenti in possesso delle amministrazioni⁹.

Il secondo fattore di complessità, cresciuto in modo particolare negli ultimi anni, è l'espansione repentina delle norme sulla digitalizzazione delle amministrazioni pubbliche. La progressiva "europeizzazione" delle regole sulla circolazione dei dati, sugli standard delle piattaforme e dei servizi online e sull'uso delle tecnologie, insieme alle norme nazionali e alle regole tecniche dell'Agenzia per l'Italia Digitale (da ora AgID), hanno reso via via più complesso il contesto normativo in cui si inserisce il lavoro dei sistemi informativi delle amministrazioni e più in generale il percorso di trasformazione digitale pubblico¹⁰.

Un insieme di norme che, in aggiunta, tende sempre ad allargare il perimetro delle tecnologie che le amministrazioni possono utilizzare nello svolgimento delle funzioni pubbliche. Emblematica è la

5. Sulle strategie di connettività nel PNRR, DEL GATTO 2022 e BUTTARELLI 2022, p. 67 ss.

6. Si v. AGID 2023, p. 7. Il corsivo utilizzato nel testo è nostro, al fine di segnalare una nuova e più precisa declinazione della trasformazione digitale che il Piano sembra dare: la nuova attenzione agli aspetti organizzativi è da valutare positivamente, considerando che questi restano fattori preliminari per la riuscita di qualsiasi percorso di innovazione pubblica. In questo senso si v. PIOGGIA 2005, p. 261 ss.

7. La letteratura sulla complessità amministrativa è ampia, ma su tutti si v. le riflessioni di ROSSI 2021, p. 37; BOMBARDELLI 2015; MOLITERNI 2017; BARBATI 2021; PIRAS 2021. Più recentemente i contributi contenuti in DE DONNO-DI LASCIO 2022.

8. Su frammentazione informativa, autonomia organizzativa e differenziazione digitale si v. per tutti MERLONI 2002. Più di recente si v. PONTI 2023; CARLONI 2023.

9. Sul potere di coordinamento informativo ed informatico dei dati come strumento di risoluzione di questo problema si v. PONTI 2008; MERLONI 2008. Più di recente CARULLO 2018; ALBERTI 2022.

10. In questo senso è emblematica l'elenco delle norme europee in questo campo attualmente vigenti contenuta in LOBASCIO 2023.

rapida crescita delle regole e delle politiche sull'utilizzo dell'intelligenza artificiale. Oltre al Regolamento (UE) 2024/1689 di recente approvazione¹¹, anche il legislatore nazionale ha introdotto o ha intenzione di introdurre nuove norme in questo ambito, ad integrazione di quelle europee: si pensi alla disciplina sull'uso di procedure automatizzate nelle gare pubbliche, contenuta nel nuovo codice dei contratti¹²; oppure al disegno di legge in materia di intelligenza artificiale in discussione in Parlamento¹³. A queste ultime poi bisogna aggiungere i numerosi documenti dedicati al tema¹⁴, da ultimo in ordine cronologico la *Strategia Italiana per l'Intelligenza Artificiale 2024-2026* appena adottata.

A questi fattori di complessità normativa e organizzativa si aggiunge un aspetto molto problematico e, fino ad ora, non sempre affrontato con la giusta costanza e consapevolezza dal legislatore europeo e nazionale: il rapporto sbilanciato tra le amministrazioni pubbliche e i poteri privati digitali che forniscono i servizi online e le tecnologie utili per la trasformazione digitale.

Da un lato, i soggetti privati forniscono alle amministrazioni gran parte delle tecnologie e delle piattaforme che queste attualmente usano per

l'erogazione di servizi online. Tecnologie e piattaforme spesso certificate e controllate dai poteri pubblici, ma in ogni caso programmate e prodotte secondo logiche e interessi diversi da quelli prettamente pubblicistici e spesso con uno standard proprietario, che incrementa il rischio di *lock-in* tecnologico delle amministrazioni stesse¹⁵. Un fattore che potrà soltanto aumentare nella sua intensità, con il progressivo utilizzo dei sistemi di intelligenza artificiale, i quali sono ad oggi prodotti prevalentemente se non esclusivamente da soggetti privati.

Inoltre, la crescita della capacità computazionale delle tecnologie algoritmiche, perlopiù in possesso dei soggetti privati, ha potenziato le loro capacità conoscitiva e, di conseguenza, la loro capacità di supportare le proprie rivendicazioni e di confrontarsi con le amministrazioni con una quantità di informazioni e di conoscenza maggiore o nettamente maggiore (come nel caso delle *big tech*)¹⁶.

Dall'altro lato, siamo in presenza di una complessiva debolezza tecnico-informatica delle amministrazioni pubbliche, frutto di numerosi fattori specifici e generali che si sono stratificati nel tempo¹⁷: il progressivo disinvestimento dei corpi

11. Facciamo riferimento al Regolamento (Ue) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale). Sulla nuova disciplina sull'intelligenza artificiale si v. ACETO DI CAPRIGLIA 2024; MARCHETTI-PARONA 2022.

12. L'art. 30 del d.lgs. 31 marzo 2023, n. 36 introduce dei principi generali sull'uso degli algoritmi nel ciclo di vita dei contratti pubblici. Per alcune riflessioni in merito si v. CARLONI 2024.

13. Si tratta del d.d.l. 1146 Disposizioni e delega al Governo in materia di intelligenza artificiale, attualmente in discussione al Senato.

14. Solo per citare le strategie e i rapporti italiani più importanti, si pensi al Libro Bianco *L'Intelligenza Artificiale a servizio del cittadino* a cura della task force IA dell'AgID nel 21 marzo 2018; al lavoro compiuto dal Ministero per lo Sviluppo Economico *Proposte per una Strategia italiana per l'intelligenza artificiale* del 2020; al *Programma Strategico per l'Intelligenza Artificiale (IA) 2022-2024* del 2021.

15. Sui rischi della fornitura di software proprietari si v. CARULLO 2020, p. 33 ss.

16. Sullo squilibrio conoscitivo tra amministrazioni e poteri privati si permetta di richiamare FALCONE 2023, pp. 23-31.

17. Da alcuni dati ricavabili dalla *Strategia nazionale per le competenze digitali*, i funzionari pubblici risultano essere anziani (il 45% dei dipendenti pubblici italiani è sopra i 54 anni contro il 22% della media OCSE) poco qualificati (solo il 38% del personale pubblico ha conseguito un titolo universitario e il 3% un titolo post-laurea) e, nonostante questo ultimo dato, scarsamente formati in ambito digitale (nel 2017, la formazione in materia di digitalizzazione ha registrato poco più di 126.000 partecipanti pari a circa il 5% del totale). Per un'analisi sulle debolezze tecnico-organizzative delle amministrazioni si v. MERLONI 2022.

tecnici a livello nazionale¹⁸; il difficile reclutamento (se non la vera e propria fuga dall'amministrazione) delle professionalità di tipo tecnico, comprese quelle informatiche¹⁹; un costante sotto-finanziamento delle amministrazioni, con importanti ricadute sulla composizione e sulla numerosità del personale; una gestione della digitalizzazione pubblica condotta con la clausola dell'invarianza finanziaria, con poca attenzione per gli aspetti organizzativi²⁰.

Queste due dinamiche hanno progressivamente definito nel tempo un rapporto privati-amministrazione pubblica fortemente sbilanciato a favore dei primi, che certifica la presenza di una sostanziale egemonia tecnologica e computazionale dei poteri privati rispetto ai poteri pubblici²¹. Tale egemonia senza dubbio costituisce un elemento di forte problematicità di un contesto già di per sé complicato.

2. La necessità di trasformare "digitalmente" le professionalità nelle amministrazioni pubbliche

Il contesto che abbiamo brevemente descritto fa emergere, tra le tante questioni che si possono intravedere, la necessità di inserire stabilmente nelle amministrazioni pubbliche conoscenze, competenze e professionalità di tipo tecnico-informatico, al fine di rendere effettiva la trasformazione digitale e reattivo il sistema amministrativo all'innovazione tecnologica²².

La moltiplicazione delle norme europee e nazionali sui dati e sulle tecnologie, la costruzione degli ecosistemi digitali, la spinta a utilizzare anche nelle

amministrazioni pubbliche i sistemi di intelligenza artificiale richiedono uno sforzo tecnico e culturale considerevole, che solo la presenza di specifiche professionalità e competenze digitali diffuse in tutto il sistema amministrativo può assicurare. Anche il riequilibrio del forte sbilanciamento in questo settore tra le amministrazioni pubbliche e i poteri privati dipende da questo elemento: la presenza di un corpo di funzionari pubblici con conoscenze e competenze digitali adeguate, capaci di contrattare meglio l'acquisto di tecnologie e piattaforme informatiche con i soggetti privati, avendo una maggiore consapevolezza delle proprie necessità e una maggiore capacità di valutazione dei prodotti che vengono offerti, e in grado di costruire degli ecosistemi digitali funzionanti, interconnessi e *data driven* è un fattore decisivo per la buona riuscita di queste politiche.

Il processo di trasformazione digitale pubblica, dunque, non passa solo dalla capacità di trasformare "digitalmente" i procedimenti amministrativi, ma in primo luogo dipende dalla capacità di trasformare "digitalmente" le professionalità nelle amministrazioni pubbliche.

Per questo motivo è emersa progressivamente nel nostro ordinamento una maggiore attenzione al rafforzamento delle competenze digitali dei funzionari pubblici²³.

Il nucleo principale attorno al quale ruotano le norme e le politiche italiane relative a questo tema è l'iniziativa strategica nazionale *Repubblica digitale*, coordinata dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri. Dal 2019, anno in cui è stato diffuso il *Manifesto per la Repubblica digitale*²⁴, la strategia ha fatto parte di

18. Sulla crisi dei corpi tecnici, si v. FIORENTINO 2013; SALTARI 2019; ZUCARO 2019.

19. Per una prospettiva sulla fuga dall'amministrazione delle professionalità tecniche si v. MELIS 2013; MELIS 2019.

20. Basti qui riportare i dati contenuti nelle *Linee di indirizzo per l'individuazione dei nuovi fabbisogni professionali da parte delle amministrazioni pubbliche 2022*, in cui è stato segnalato come «al 1° gennaio 2021, il comparto contava 3,2 milioni di dipendenti, 31 mila in meno rispetto all'anno precedente (-0,97%, il minimo storico degli ultimi 20 anni), di età avanzata (in media 50 anni)». Sulle politiche di contenimento della spesa pubblica e sui suoi effetti sul sistema amministrativo si v. MERLONI 2018.

21. Sull'emergere di una egemonia computazionale dei poteri privati si permetta di richiamare le considerazioni in FALCONE 2023, pp. 28-29.

22. Per una riflessione in merito si v. ACOCELLA-DI MARTINO 2022.

23. Per una ricostruzione sulla formazione e sul reclutamento nel PNRR si v. SGUEO 2022.

24. Attorno al manifesto, proposto dall'allora Team per la trasformazione digitale, si è formata la *Coalizione Nazionale per le competenze digitali*, formata da tutti coloro che hanno sottoscritto il [manifesto](#). Dal 2020 la Coalizione ha aderito alla *Digital Skills and Jobs Coalition* europea, una coalizione di livello europeo che mobilita enti e

tutte le politiche di digitalizzazione che si sono succedute negli anni: inaugurata di fatto con 2025: *Piano Nazionale per l'Innovazione*, poi divenuto *Italia 2025. Strategia per l'innovazione tecnologica e la digitalizzazione del Paese 2025*, fino al suo inserimento e al suo maggiore finanziamento con il PNRR.

Ovviamente *Repubblica digitale* ha degli obiettivi di più ampio respiro: è un'iniziativa strategica partecipata – a cui aderiscono istituzioni, imprese e associazioni – che ha come obiettivo quello di ridurre il divario digitale dell'Italia rispetto agli altri Paesi europei, favorendo la crescita delle competenze digitali non solo dei funzionari pubblici, ma di tutti i cittadini italiani²⁵.

In ogni caso, le principali iniziative legislative e i documenti di indirizzo politico-amministrativo più importanti sul rafforzamento delle competenze digitali dei funzionari, in particolare dopo l'approvazione del PNRR, sono state previste nell'ambito di questa strategia.

2.1. Le indicazioni normative sulle competenze digitali dei funzionari

A livello legislativo, sono poche le norme che hanno richiamato (anche se timidamente) la necessità

di specifiche professionalità nelle amministrazioni pubbliche. Il legislatore nazionale ha concentrato la sua attenzione su tre ambiti: un semplice richiamo alle competenze di particolari figure organizzative, come il Responsabile per la transizione digitale (da ora RTD); alcuni indirizzi generali sulla pianificazione dei fabbisogni professionali delle amministrazioni; il finanziamento della strategia *Repubblica digitale*, nell'ambito degli interventi sul PNRR.

Nel primo caso, facciamo riferimento alla disciplina del RTD. Questa figura, ricordiamolo, è stata prevista con il d.lgs. 13 dicembre 2017, n. 217, che ha modificato la rubrica dell'art. 17 del d.lgs. 7 marzo 2005, n. 82, al fine di imprimere un'accelerazione all'attuazione e all'effettività delle disposizioni previste nel Codice dell'amministrazione digitale nel sistema amministrativo. Per i nostri fini, è interessante il comma 1-ter dell'art. 17 – come modificato dal d.lgs. 26 agosto 2016, n. 179 – il quale afferma che il RTD debba avere «adeguate competenze tecnologiche, di informatica giuridica e manageriali». Tre tipi di competenze che, nella visione del legislatore, dovrebbero essere quelle più adeguate per dirigere l'ufficio interno alle amministrazioni che è stato individuato per l'esercizio della funzione di digitalizzazione pubblica²⁶.

organizzazioni degli Stati membri, per garantire che tutti i cittadini europei acquisiscano le competenze digitali di cui hanno bisogno.

25. La regia dell'iniziativa è affidata al Comitato tecnico guida, coordinato dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri. A questo Comitato partecipano i Ministeri (Cultura; Istruzione e Merito; Lavoro e Politiche sociali; Famiglia, Natalità e Pari opportunità; Agricoltura, Sovranità alimentare e Foreste; Sport e Giovani; Pubblica Amministrazione; Imprese e Made in Italy; Università e Ricerca), la Conferenza delle regioni, l'Unione province italiane (UPI), l'Associazione nazionale comuni italiani (Anci), l'Agenzia per l'Italia digitale (AgID), Unioncamere, esponenti del mondo dell'Università (Conferenza dei Rettori delle università italiane e il coordinatore della EU Code Week), della ricerca (Consulta dei Presidenti degli enti di ricerca), della RAI, di Confindustria digitale e di associazioni di cittadini della Coalizione Nazionale per le competenze digitali.
26. Per essere più precisi, la stessa disposizione prevede che il RTD abbia le seguenti competenze: «a) coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni; b) indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione; c) indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1; d) accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4; e) analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa; f) cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e); g) indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia; h) progettazione e coordinamento delle

Una disposizione che aveva come obiettivo principale quello di indirizzare le nomine dei Responsabili nelle amministrazioni verso figure con un adeguato profilo professionale, ma il risultato ad oggi non ha raggiunto quanto sperato.

Il *Piano triennale per l'informatica nelle pubbliche amministrazioni 2024-2026* ha segnalato come «a novembre 2023, analizzando i dati disponibili sull'Indice dei domicili digitali della Pubblica Amministrazione e dei Gestori di Pubblici Servizi, risultano ancora da nominare circa 2.400 RTD nelle pubbliche amministrazioni e negli enti pubblici con tale obbligo di nomina». Il Piano segnala anche che il trend delle nomine è in crescita, in particolare grazie alla scelta di molte amministrazioni locali di «procedere alla nomina del RTD e alla costituzione dell'Ufficio per la transizione digitale in forma associata, in aderenza a quanto previsto dal comma 1-septies dell'art. 17 del CAD»²⁷.

L'aspetto critico, oltre alla lentezza della nomina di questa figura nelle amministrazioni, è il profilo professionale dei responsabili. Secondo il Piano triennale alcune di queste figure nelle amministrazioni comunali sono ricoperte dai segretari comunali, i quali tradizionalmente non hanno il tipo di competenze richieste dall'art. 17. Ad oggi non abbiamo dati aggregati e aggiornati sui profili professionali che ricoprono l'incarico di Responsabile per la transizione digitale, ma gli ultimi dati disponibili non erano confortanti. La Relazione finale della Commissione di inchiesta parlamentare sulla

digitalizzazione ha messo in evidenza come «degli otto responsabili nominati dai Ministeri ai sensi dell'articolo 17, uno solamente è risultato essere in possesso di un titolo di istruzione superiore coerente col ruolo ricoperto, nel caso specifico laurea in ingegneria informatica; negli altri sette casi, cinque delle figure nominate sono risultate in possesso di una laurea in giurisprudenza, una della laurea in medicina e chirurgia ed una del titolo in ingegneria civile. Con riferimento, invece, alle amministrazioni regionali, solo due nomine delle sette totali erano state operate in ossequio ai requisiti sul possesso della laurea informatica richiesta dal Codice dell'amministrazione digitale, mentre delle cinque nomine relative alle città metropolitane, soltanto una rispettava i suddetti requisiti»²⁸.

Oltre alle disposizioni dedicate al RTD, il legislatore è tornato anche ad occuparsi dell'effettivo fabbisogno professionale delle amministrazioni, provando a indirizzare e a coordinare la pianificazione e la programmazione delle assunzioni nelle amministrazioni pubbliche, indicando *ex lege* criteri che privilegino il reclutamento di personale con specifiche competenze, anche digitali.

Come è noto, sulla base della delega contenuta nella legge 7 agosto 2015, n. 124²⁹, il d.lgs. 25 maggio 2017, n. 75 ha introdotto l'articolo 6-ter al d.lgs. 30 marzo 2001, n. 165, in cui si prevede che il Ministro per la pubblica amministrazione, di concerto con il Ministro dell'economia e delle finanze, definisce, nel rispetto degli equilibri di finanza pubblica, le

iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi; i) promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie; j) pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione e quello di cui all'articolo 64-bis; j-bis) pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale di cui all'articolo 16, comma 1, lettera b)».

27. Per entrambe le citazioni si v. AGID 2023, p. 20.

28. Così Commissione parlamentare di inchiesta sul livello di digitalizzazione e innovazione delle Pubbliche Amministrazioni e sugli investimenti complessivi riguardanti il settore delle tecnologie e della comunicazione, *Relazione sull'attività svolta*, cit., p. 95.

29. La legge, tra i diversi principi di delega, all'art. 17 delinea un approccio al governo delle risorse umane basato sui concetti di "fabbisogno di personale" e di "rilevazione delle competenze dei lavoratori pubblici".

linee di indirizzo per orientare le amministrazioni pubbliche nella predisposizione dei rispettivi Piani dei fabbisogni di personale³⁰.

Un potere di indirizzo che il legislatore ha progressivamente definito nel dettaglio, a partire dalla legge 19 giugno 2019, n. 56³¹, fino alla legge 29 giugno 2022, n. 79 di conversione del d.l. 30 aprile 2022, n. 36, con lo scopo di portare le singole amministrazioni ad individuare soprattutto i «fabbisogni prioritari o emergenti» e a reclutare funzionari rispondenti ai «nuovi profili professionali individuati dalla contrattazione collettiva, con particolare riguardo all'insieme di conoscenze, competenze e capacità del personale da assumere anche *per sostenere la transizione digitale ed ecologica della pubblica amministrazione* e relative anche a strumenti e tecniche di progettazione e partecipazione a bandi nazionali ed europei, nonché alla gestione dei relativi finanziamenti»³².

Leggendo le prime due *Linee di indirizzo per l'individuazione dei nuovi fabbisogni professionali da parte delle amministrazioni pubbliche* – adottate una con il d.m. 8 maggio 2018 e l'altra, più recentemente, con il d.m. 22 luglio 2022 – non ci sono però indicazioni specifiche sulle conoscenze, sulle competenze e sulle capacità digitali che dovrebbero avere i funzionari o una specificazione dei profili professionali utili alla trasformazione digitale. Questo non significa che di per sé le linee di indirizzo siano inutili, anzi. Da una lettura dei due testi, in particolare il secondo, emerge molto bene

la volontà del Dipartimento (nonostante i differenti colori politici dei governi in cui esse sono state approvate) di formalizzare in più fasi il processo di ricostruzione del fabbisogno per le singole amministrazioni. Una formalizzazione non cogente, ovviamente, ma solo descrittiva, che però costituisce un interessante tentativo di costringere le amministrazioni a riflettere sui propri fabbisogni e sui metodi per soddisfarli, anche relativamente alla trasformazione digitale.

Lo stesso approccio è riscontrabile nei due rapporti elaborati dall'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (da ora Aran) e il Dipartimento della Funzione pubblica *Metodi di analisi di fabbisogni di personale, professioni e competenze* e *Modello di rappresentazione delle professioni e competenze nelle PpAa* del novembre 2017. Entrambi i documenti hanno tentato di proporre metodi di analisi e classificazioni di competenze e di professionalità in grado di coadiuvare il lavoro sui fabbisogni delle singole amministrazioni, ma non hanno dedicato uno spazio specifico alle competenze e alle professionalità digitali.

Infine, anche la legislazione dedicata all'attuazione del PNRR, ad oggi il principale strumento per la trasformazione digitale delle amministrazioni, contiene solo alcuni riferimenti generali sulle competenze digitali, non specificamente riferite ai funzionari pubblici, ma in ogni caso utili ai fini della strategia *Repubblica digitale*³³. Tra queste disposizioni italiane di attuazione, si avvicinano

30. Con riferimento al Piano triennale dei fabbisogni di personale, si rammenta che, per effetto dell'art. 6 del d.l. 9 giugno 2021, n. 80, esso è confluito nel Piano integrato di attività e organizzazione (PIAO), quale strumento unico di coordinamento che mette in correlazione la programmazione dei fabbisogni di risorse umane – espressa in termini di profili professionali e competenze – alla programmazione strategica dell'ente e alle strategie di valorizzazione degli obiettivi di interesse pubblico.

31. La legge ha disposto all'art. 3, comma 2, che il Piano dei fabbisogni venga predisposto tenendo conto dell'esigenza di reclutare figure professionali con elevate competenze, tra cui, quelle digitali. Testualmente «2. Al fine di accrescere l'efficienza dell'organizzazione e dell'azione amministrativa, le amministrazioni di cui al comma 1 predispongono il piano dei fabbisogni di cui agli articoli 6 e 6-ter del decreto legislativo n. 165 del 2001, tenendo conto dell'esigenza di assicurare l'effettivo ricambio generazionale e la migliore organizzazione del lavoro, nonché, in via prioritaria, di reclutare figure professionali con elevate competenze in materia di: a) *digitalizzazione*; b) razionalizzazione e semplificazione dei processi e dei procedimenti amministrativi; c) qualità dei servizi pubblici; d) gestione dei fondi strutturali e della capacità di investimento; e) contrattualistica pubblica; f) controllo di gestione e attività ispettiva; g) contabilità pubblica e gestione finanziaria.». Il corsivo è il nostro.

32. Il corsivo è nostro.

33. Nella legislazione europea e nazionale che disciplina il PNRR, le disposizioni normative sono dedicate principalmente al rafforzamento delle competenze digitali nelle istituzioni scolastiche. In questo senso il Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021, che istituisce uno strumento

al tema che stiamo trattando le nuove norme sul reclutamento e sulla selezione della dirigenza pubblica, in particolare le nuove *Linee guida sull'accesso alla dirigenza pubblica*, adottate sempre dal Dipartimento della Funzione pubblica, e le norme che istituiscono il Fondo dedicato alla strategia *Repubblica digitale*.

L'art. 3 del d.l. 9 giugno 2021, n. 80, come modificato dal d.l. 30 aprile 2022, n. 36, ha a sua volta modificato l'art. 28, comma 1-*bis* del d.lgs. 30 marzo 2001, n. 165 che disciplina l'accesso alla dirigenza di seconda fascia. Questa modifica prevede che, oltre all'accertamento delle conoscenze delle materie previste dalla legge, nelle procedure concorsuali per l'accesso alla dirigenza si debbano valutare anche le capacità, le attitudini e le motivazioni individuali dei candidati. Un arricchimento della valutazione che deve essere prevista espressamente nei bandi attraverso l'individuazione degli ambiti di competenza che devono essere valutati in sede concorsuale. In attuazione di questa disposizione il comma 6 dell'art. 3 del d.l. 9 giugno 2021, n. 80 prevede che «il Ministro per la pubblica amministrazione, acquisite le proposte della Scuola nazionale dell'amministrazione, entro il 31 ottobre 2022, con proprio decreto, previa intesa in sede di Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, adotta specifiche linee guida».

Le *Linee guida sull'accesso alla dirigenza pubblica* sono state effettivamente adottate con l'obiettivo di «declinare in indicazioni operative i principi

fondamentali dettati in materia dalla nuova normativa sul reclutamento al fine di assicurare l'omogeneità di operato delle amministrazioni in questo ambito». Queste indicazioni contengono un nuovo paradigma di riferimento per orientare le metodologie, le tecniche e le procedure che governano l'accesso alle qualifiche dirigenziali del sistema amministrativo, ma non contengono indicazioni specifiche dedicate all'accertamento delle competenze digitali dei dirigenti.

Oltre allo sviluppo delle competenze digitali dei docenti³⁴, il d.l. 6 maggio 2021, n. 59, convertito con modificazioni dalla legge 1° luglio 2021, n. 101, ha istituito e finanziato il Fondo per la *Repubblica digitale*³⁵, dedicato «al sostegno di progetti rivolti alla formazione e all'inclusione digitale, con la finalità di accrescere le competenze digitali, anche allo scopo di migliorare i corrispondenti indicatori del Digital Economy and Society Index (DESI) della Commissione europea»³⁶.

2.2. Le politiche sulla diffusione delle competenze digitali nel sistema amministrativo

Al di là delle previsioni normative appena richiamate, il cuore delle politiche sulle competenze digitali dei funzionari sono gli indirizzi politico-amministrativi di attuazione dell'iniziativa strategica *Repubblica digitale* presenti nella *Strategia nazionale per le competenze digitali* e nel correlato Piano operativo, adottata dal Comitato tecnico guida, le

di sostegno tecnico, definito all'art. 2 come «misure che aiutano le autorità nazionali ad attuare riforme istituzionali, amministrative e strutturali che siano sostenibili, rafforzino la resilienza, potenzino la coesione economica, sociale e territoriale e sostengano la pubblica amministrazione nella preparazione di investimenti sostenibili e capaci di rafforzare la resilienza». Secondo queste disposizioni uno degli obiettivi dello strumento tecnico è il rafforzamento delle competenze digitali nella scuola. Anche il Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021 che istituisce il dispositivo per la ripresa e la resilienza (come modificato da ultimo dal Regolamento (UE) 2024/795 del Parlamento europeo e del Consiglio) prevede il rafforzamento di competenze digitali nei percorsi di istruzione o di formazione nel Capo III *bis*, dedicato al Piano REPowerEU, nella disciplina sugli Orientamenti per la valutazione del dispositivo e nell'Allegato V del regolamento.

34. Si v. in particolare il comma 1 dell'art. 24-*bis*, il quale, per lo sviluppo delle competenze digitali, prevede la definizione di percorsi formativi digitali, a decorrere dall'anno scolastico 2022/2023 e per un triennio, nel Piano nazionale di formazione dei docenti delle scuole di ogni ordine e grado.

35. In particolare l'art. 29 afferma che «Nell'ambito dell'intervento "Servizi digitali e competenze digitali" del Piano nazionale per gli investimenti complementari di cui all'articolo 1, comma 2, lettera a), numero 2), del decreto-legge 6 maggio 2021, n. 59, convertito, con modificazioni, dalla legge 1° luglio 2021, n. 101, in via sperimentale, per gli anni 2022, 2023, 2024, 2025 e 2026, è istituito il "Fondo per la Repubblica Digitale"».

36. In questo senso il comma 2 dell'articolo ivi richiamato.

organizzazioni partner e la Coalizione nazionale di Repubblica digitale.

La *Strategia nazionale per le competenze digitali* contiene gli interventi organici e multisettoriali per migliorare le competenze digitali del Paese con il duplice fine di eliminare il dislivello con gli altri Paesi europei³⁷ e di abbattere il *digital divide* tra varie aree del nostro territorio nazionale.

Tra gli assi principali³⁸, quello dedicato alla forza lavoro attiva contiene gli interventi sulle competenze dei funzionari pubblici. Questo asse è stato predisposto in via generale per garantire le competenze digitali adeguate nel mondo del lavoro, sia nel settore privato, sia nel settore pubblico. In questo ultimo caso ha previsto una serie di interventi spesso dedicati a platee di funzionari differenti: dirigenti pubblici, specialisti IT e funzionari e dipendenti pubblici.

Il primo tipo di interventi che è confluito nella Strategia, anche se precedenti ad essa, sono le *Linee guida per la qualità delle competenze digitali nelle professionalità ICT* e le *Linee guida per l'armonizzazione delle qualificazioni professionali*, entrambe adottate dall'AgID. Con questi due documenti l'Agenzia ha definito e sistematizzato le competenze e le professionalità digitali in funzione del diverso ruolo che queste possono assumere nel processo di attuazione della trasformazione digitale

nelle amministrazioni. Un lavoro utilissimo, ma che sembra più una guida per le amministrazioni a quale figura esterna contrattualizzare o a che tipo di clausole tecniche inserire nei bandi ad oggetto tecnologico, più che un vademecum su quale tipo di figure reclutare o formare e per quale tipo di finalità generali.

Una parte importante degli interventi è dedicata alla delineazione dei fabbisogni e dei contenuti formativi dei funzionari e, in particolare, della figura del RTD. Nel tempo l'AgID ha confezionato, confermandoli anche in questa versione del Piano operativo, dei cicli di webinar formativi su innovazione e amministrazioni pubbliche (come ad esempio, i “Cicli di formazione AGID-CRUI per Responsabili per la Transizione al Digitale - RTD – Webinar”) e delle attività laboratoriali per rispondere alle nuove richieste delle amministrazioni territoriali in relazione ai temi della digitalizzazione pubblica (come i “Laboratori formativi specialistici per lo sviluppo di attività individuate dalla community dei RTD”).

Inoltre, nell'Asse 2.2. del Piano operativo della *Strategia nazionale per le competenze digitali* sono previsti altri interventi formativi più generali, rifinanziati ed estesi con il PNRR, in cui rientrano anche quelli esplicitamente dedicati all'utilizzo dei digitali³⁹: ad esempio il “rafforzamento delle

37. È utile riportare i dati sul divario italiano rispetto alla media europea che la medesima Strategia segnala come punto di partenza della sua azione. Secondo la Strategia «il 58% della popolazione italiana tra i 16 e i 74 anni (26 milioni di cittadini) non ha le competenze digitali di base – rispetto al 42% della media dell'Unione europea –, e, di questi, 11 milioni non sono utenti di Internet. Solo il 22% della popolazione possiede competenze digitali superiori al livello base. Sul totale della popolazione laureata, solo 1 individuo su 100 ha conseguito una laurea in ICT. Con riferimento alla popolazione femminile, la percentuale scende drasticamente allo 0,3%. Il divario di genere tra individui in possesso di un titolo di studio elevato con competenze digitali avanzate è del 13%. 6,75% lavoratori sia nel settore privato che in quello pubblico hanno competenze digitali superiori al livello base».

38. Oltre all'asse richiamato nel testo la Strategia è formata da altri tre assi: uno dedicato all'istruzione e formazione superiore per lo sviluppo delle competenze digitali all'interno dei cicli d'istruzione formale per i giovani, con il coordinamento del Ministero dell'Istruzione (MI) e del Ministero dell'Università e della Ricerca (MUR); uno dedicato alle competenze specialistiche ICT, per potenziare la capacità del Paese di sviluppare competenze per nuovi mercati e nuovi lavori, in gran parte legati alle tecnologie emergenti e al possesso delle competenze chiave per i lavori del futuro, con il coordinamento di Ministero dell'Università e Ricerca (MUR) e Ministero dello Sviluppo Economico (MISE); uno dedicato alle competenze digitali dei cittadini, per sviluppare le competenze digitali necessarie a esercitare i diritti di cittadinanza e la partecipazione consapevole alla vita democratica, con il coordinamento del Ministro per l'Innovazione tecnologica e la Digitalizzazione (MID).

39. Interventi che rientrano in assi diversi del PNRR come: M1C1 I2.3 “Competenze: Competenze e capacità amministrativa”; M1C1 I2.3.1 “Investimenti in istruzione e formazione”; M1C3I 1.1.6 “Formazione e miglioramento delle competenze digitali”; M4C1 I4.1 “Estensione del numero di dottorati di ricerca e dottorati innovativi per la pubblica amministrazione e il patrimonio culturale”.

competenze manageriali a supporto della transizione digitale” promosso dalla SNA; oppure l'introduzione di misure per favorire il rafforzamento delle competenze e l'iscrizione dei dipendenti pubblici alla formazione terziaria, inclusi percorsi dedicati alla trasformazione digitale (il progetto “PA 110 e Lode”); la realizzazione di attività volte a migliorare la capacità amministrativa delle amministrazioni locali per la riorganizzazione digitale dei processi (ad esempio, il “Progetto FAST: capacità delle PA locali nell'attuazione di interventi di semplificazione e organizzazione in chiave digitale”).

Una particolare attenzione tra le attività formative merita il Progetto *Competenze digitali per la PA*, un progetto promosso dal Dipartimento della funzione pubblica nell'ambito del PON Governance e Capacità Istituzionale 2014-2020, che punta a costruire dei piani formativi personalizzati per accrescere le competenze in ambito digitale dei funzionari pubblici sulla base di un *Syllabus “Competenze digitali per la PA”*, ispirato all'impianto del framework europeo sulle competenze di cittadinanza digitale (DigComp)⁴⁰.

I documenti prodotti in questo progetto sono gli unici che provano ad individuare, seppure solo a fini formativi, quali debbano essere i contenuti delle competenze digitali dei funzionari pubblici nell'esercizio delle funzioni pubbliche.

Le competenze digitali dei funzionari vengono divise in quattro tipologie: le competenze digitali di base; le competenze digitali specialistiche; le competenze digitali complementari; le competenze digitali manageriali o di *e-leadership*.

Le competenze digitali di base sono quelle volte principalmente ad assicurare a tutti i funzionari e dipendenti pubblici l'utilizzo appropriato degli strumenti informatici e tecnologici a supporto dell'ufficio di appartenenza: parliamo di conoscenze di base su tecnologie e dati; di capacità di comunicazione e di creazione di contenuti digitali; di capacità di applicazione delle norme basi sulla

sicurezza informatica; delle abilità di risolvere problemi degli strumenti che si utilizzano durante l'azione amministrativa.

Le competenze digitali specialistiche, invece, sono quelle prettamente tecniche, necessarie a fronteggiare la progressiva diffusione di tecnologie complesse in ambito pubblico, come ad esempio i sistemi di intelligenza artificiale o, comunque, le tecnologie computazionali di nuova generazione. Competenze che, secondo questi documenti, sono frutto di percorsi formativi e professionali che non possono essere acquisite solo con la formazione, ma attraverso la selezione e la valorizzazione di nuove figure professionali nelle amministrazioni pubbliche.

La trasformazione digitale richiede, poi, anche competenze digitali complementari, cioè capaci di abilitare i funzionari ad attuare, con padronanza e dimestichezza, i cambiamenti apportati dalle tecnologie digitali nei procedimenti e nell'organizzazione di un'amministrazione. Le tecnologie non sono mai solo degli strumenti tecnici, ma spesso il loro utilizzo tende a rendere superflue o ridondanti determinate prassi procedurali o richiede qualche cambiamento organizzativo. Le competenze complementari sono, di fatto, quelle che dovrebbero servire a produrre questi cambiamenti.

Infine, di fondamentale importanza sono le competenze digitali manageriali o di *e-leadership*, in capo alle figure dirigenziali. Competenze di questo tipo sono determinanti per guidare la trasformazione digitale di strutture complesse come sono le amministrazioni. A dimostrazione della loro rilevanza sono state adottate anche specifiche *Linee guida di eLeadership*, adottate dal Dipartimento della Funzione pubblica.

In sintesi, i dirigenti pubblici, oltre alle c.d. *soft skills*⁴¹, devono avere una cultura digitale solida, cioè devono possedere una cultura e delle conoscenze diffuse sul mondo digitale e, in modo particolare, sui sistemi informatici e tecnologici che sono

40. Il *Syllabus “Competenze digitali per la PA”*, strutturato in cinque aree di competenza e tre livelli di padronanza, rappresenta la base di riferimento per uno strumento di *self-assessment* on-line delle conoscenze e abilità possedute (<http://www.competenzedigitali.gov.it>) che consente di rilevare i propri fabbisogni formativi, di accedere ad una offerta di corsi mirata e gratuita e di misurare i propri progressi. L'offerta formativa in *e-learning*, organizzata in un Catalogo corsi, è resa disponibile insieme allo strumento di *self-assessment* a tutte le amministrazioni che decidono di aderire all'iniziativa.

41. Per *soft skill* si intendono quelle capacità individuali dei dirigenti di relazionarsi e di comunicare efficacemente con il personale del proprio ufficio o con gli organi politici.

in uso nel settore pubblico; devono avere abilità di leadership organizzativa, cioè devono essere in grado di organizzare o riorganizzare la propria amministrazione o il proprio ufficio, tenendo presente i cambiamenti presupposti dall'utilizzo di strumenti tecnologici; infine, devono conoscere i processi digitali delle amministrazioni di appartenenza e del sistema amministrativo e devono essere in grado di individuare trend e capire quali saranno le possibili applicazioni utili alla propria organizzazione.

3. L'esigenza di essere più coraggiosi: la necessità di una riflessione organica su competenze, professionalità e organizzazione del digitale

Le disposizioni che abbiamo richiamato e l'iniziativa strategica *Repubblica digitale*, insieme ai vari progetti e alle varie strategie che in essa sono confluite, dimostrano senza dubbio la volontà del legislatore e dell'indirizzo politico-amministrativo di provare a definire politiche pubbliche atte a migliorare le competenze digitali dei funzionari pubblici.

Il *Progetto Competenze digitali per la PA*, con il relativo *Syllabus*, e le *Linee guida di eLeadership*, in particolare, contengono i risultati di una prima riflessione istituzionale su quali conoscenze e competenze, su quali tipi di professionalità servono alle amministrazioni pubbliche. Una riflessione che ha provato a ragionare per ruoli organizzativi – dividendo le competenze necessarie alla dirigenza pubblica (in particolare al ruolo di RTD), ai tecnici delle amministrazioni, ai semplici funzionari e dipendenti pubblici – e in un'ottica di medio-lungo periodo: se si incrociano queste considerazioni sulle competenze digitali dei funzionari pubblici con gli indirizzi iniziali del Dipartimento della Funzione pubblica sulla programmazione del fabbisogno di personale, sulla selezione della dirigenza e sul raggiungimento degli obiettivi formativi anche in materia digitale, si delinea di fatto un programma di medio-lungo periodo.

La complessità e le problematicità di cui abbiamo parlato, d'altronde, possono essere “governate” solo con la progressiva formazione e introduzione nelle amministrazioni o nel sistema amministrativo di specifiche professionalità – che predispongano

e connettano “tecnicamente” le amministrazioni e che attuino le regole tecniche dell'AgID –, di competenze manageriali digitali – capaci di guidare concretamente la trasformazione digitale delle amministrazioni –, di competenze digitali diffuse nei funzionari pubblici. Un insieme di elementi che possano abilitare concretamente questi ultimi alla comprensione del funzionamento tecnico-pratico delle tecnologie utilizzate e utilizzabili, come l'intelligenza artificiale, della logica “tecnologica” e *data-driven* dell'ecosistema digitale che sta emergendo progressivamente nelle intenzioni dei legislatori e dei governi. Una necessità che diventa una priorità, se consideriamo la dipendenza delle amministrazioni dai poteri privati in termini di tecnologie e di capacità computazionale.

Nonostante questi elementi positivi, però, l'approccio del legislatore e dell'indirizzo politico-amministrativo degli ultimi anni in materia di competenze digitali risulta problematico da più punti di vista.

In primo luogo, è un approccio che risulta essere troppo appiattito sulla formazione professionale del personale pubblico, anziché su una strategia integrata che affianchi quest'ultima al reclutamento di nuovi funzionari e di nuove professionalità.

La formazione, da sola, non può colmare il gap generazionale e culturale in materia digitale di un apparato amministrativo molto anziano, né può garantire stabilmente conoscenze e competenze utili per una complessiva trasformazione digitale. Questi obiettivi passano, invece, da una programmazione del fabbisogno del personale strategica e da risorse economiche adeguate per il reclutamento di nuove professionalità nelle amministrazioni⁴².

Se in merito alla programmazione dei fabbisogni e alle regole di selezione della dirigenza pubblica qualcosa è stato fatto – anche se in via troppo generale e senza una reale attenzione ai fabbisogni “digitali” delle amministrazioni –, sul reclutamento in sé per sé il quadro è in chiaroscuro, principalmente a causa della mancanza di risorse economiche adeguate. In via generale le regole sull'utilizzo delle risorse del PNRR vietano il loro utilizzo per il reclutamento di personale a tempo indeterminato e le risorse per le assunzioni a tempo determinato non sono state fino ad ora sufficienti per

42. Per alcune riflessioni alternative e critiche rispetto al contesto normativo in vigore si v. AVERARDI-SAN MAURO 2019; STACCA 2019.

attirare professionalità nel sistema amministrativo, in particolare nelle amministrazioni che ne avevano maggiormente bisogno, come quelle di piccole dimensioni e del Sud Italia. Nell'ultimo anno il governo ha deciso di avviare una selezione di tecnici da assumere a tempo indeterminato, tra cui specialisti informatici, per le amministrazioni meridionali, utilizzando però i fondi delle politiche europee di coesione⁴³. Inoltre, il Dipartimento per la trasformazione digitale ha istituito il *Transformation Office*, un ufficio di tecnici assunti per sostenere la transizione digitale delle amministrazioni, in particolare di quelli territoriali⁴⁴. Al di là di queste due iniziative, una politica stabile e incrementale di assunzioni mirate alla trasformazione digitale non sembra ancora emergere in modo efficace.

In secondo luogo, l'individuazione delle abilità e delle competenze digitali, non sembra avere il respiro adeguato a una innovazione tecnologica sempre più repentina e sempre più centrata su tecnologie, come i sistemi di intelligenza artificiale, basate sulla gestione dei dati in possesso delle amministrazioni, sempre più *data-driven*.

I documenti che abbiamo segnalato non ignorano questo elemento: tra le competenze e le abilità segnalate, i big data, gli algoritmi, più in generale la gestione dei dati per la loro computazione vengono spesso richiamate tra le competenze specialistiche e quelle manageriali, ma non sono mai messe realmente a sistema.

La mancanza di sistematicità e di organicità delle competenze digitali dei funzionari nel sistema amministrativo, infatti, è il terzo elemento problematico che è possibile segnalare da questa ricostruzione.

L'individuazione delle competenze digitali è avvenuta senza una visione d'insieme dell'assetto professionale e della struttura organizzativa delle amministrazioni o delle tecnologie largamente in

uso al loro interno. Anteporre una riflessione sui fabbisogni del personale, sulle competenze digitali dei funzionari, senza riflettere preliminarmente o contestualmente sull'assetto organizzativo delle funzioni coinvolte da questi processi (come quella conoscitiva, quella informativa e quella di digitalizzazione), rischia di essere un lavoro lontano dalla realtà amministrativa su cui si vorrebbe intervenire.

Dall'analisi che abbiamo compiuto, dunque, emerge la necessità di affrontare il tema delle competenze digitali delle amministrazioni in modo più coraggioso.

In un modo cioè che, da un lato, integri la precisa individuazione di singole competenze o abilità digitali necessarie per modernizzare le amministrazioni con una visione di insieme, basata su una vera cultura dell'amministrare con i dati e, dall'altro lato, rifletta anche sulla dimensione organizzativa di queste competenze, cioè rifletta sul modo più adeguato e più coerente per valorizzare le competenze statistiche decentrate, quelle informatiche e informative e quelle recentemente affidate all'ufficio del Responsabile per la trasformazione digitale, nelle amministrazioni.

4. Una prospettiva alternativa: la *data science* come nuovo sapere per governare le intelligenze artificiali

Oggi, una prospettiva differente, che potrebbe integrare efficacemente l'approccio che il legislatore e l'indirizzo politico-amministrativo hanno avuto fino ad ora, ma con una finalità più generale, cioè non solo quella di trasformare i procedimenti amministrativi, ma di governare le intelligenze artificiali pubbliche in futuro, dovrebbe partire da una valutazione complessiva dei saperi presenti nelle amministrazioni. In particolare, i saperi che potrebbero gestire dati e informazioni in un'ottica *data-driven*, a partire dai saperi che tradizionalmente si sono occupati delle specifiche funzioni

43. Ci riferiamo all'*Avviso pubblico finalizzato alla acquisizione delle manifestazioni di interesse da parte delle amministrazioni regionali della Basilicata, Calabria, Campania, Molise, Puglia, Sardegna e Sicilia, e delle città metropolitane, delle province, delle unioni di comuni e dei comuni ivi situati* per l'assunzione di personale tecnico a tempo indeterminato presso i principali beneficiari. Un avviso, chiuso il 30 gennaio 2024, rientrante nel *Programma Nazionale di Assistenza Tecnica "Capacità per la Coesione" 2021-2027* (PN CapCoe).

44. Oltre ad un nucleo centrale, la struttura è dislocata su tutto il territorio attraverso dei team territoriali, organizzati su 6 macro aree locali: Nord est (Emilia-Romagna, Veneto, Friuli-Venezia Giulia, Trentino-Alto Adige); Lombardia; Nord ovest (Piemonte, Liguria, Valle D'Aosta); Centro (Lazio, Toscana, Marche, Umbria, Sardegna); Sud ovest (Campania, Calabria, Sicilia); Sud est (Puglia, Basilicata, Abruzzo, Molise).

amministrative che hanno come loro principale oggetto di lavoro il dato.

Nelle amministrazioni pubbliche già oggi il sapere informatico e quello ingegneristico caratterizzano da tempo la funzione informativa⁴⁵, così come il sapere statistico caratterizza la funzione statistica, una delle principali funzioni conoscitive del nostro ordinamento⁴⁶.

Questi saperi, però, non sembrano essere adatti, da soli, al governo delle informazioni e della conoscenza non convenzionale che la *big data analytics* produce nel processo decisionale o alla gestione delle elaborazioni algoritmiche dei sistemi di intelligenza artificiale⁴⁷. Vero è che la statistica, l'ingegneria e l'informatica oggi si confrontano stabilmente con la rivoluzione dei dati e le professionalità che hanno questa formazione molte volte sono in grado di utilizzare gli strumenti di *data analytics* o di intelligenza artificiale, ma lo fanno all'interno dei propri specifici aspetti tecnico-scientifici: la statistica per gli aspetti più metodologici, l'informatica e l'ingegneria per gli aspetti più architetturali. Le particolari caratteristiche dei dati e della conoscenza prodotta, necessitano di competenze specifiche, che non solo permettano un felice intreccio dei saperi tradizionali che abbiamo appena elencato, necessari ma non (auto)sufficienti nella rivoluzione dei dati, ma che sappiano introdurre una nuova cultura della gestione del dato nel e per il processo decisionale⁴⁸.

Queste due caratteristiche, essere collante tra i saperi tradizionali e avere un nuovo approccio manageriale ai dati e al loro utilizzo a fini decisionali, costituiscono il nucleo principale della *data science*: un nuovo sapere tecnico che è necessario introdurre capillarmente all'interno

delle amministrazioni pubbliche, se davvero queste volessero utilizzare a pieno e responsabilmente le potenzialità della rivoluzione dei dati.

La scienza dei dati è una disciplina trasversale, a cui fanno capo sia le sfere dell'informatica, della statistica e della matematica, sia un insieme di competenze più manageriali, legate alla più recente necessità di sapere leggere, interpretare e valorizzare i dati. La *data science* assume carattere scientifico autonomo nel 2001⁴⁹ ed è caratterizzata da un processo analitico regolato da una serie di principi metodologici, basati sul metodo scientifico, e di tecniche multidisciplinari⁵⁰ volti ad estrarre informazioni e conoscenza nuova dai dati, ad interpretarla e a utilizzarla nel processo decisionale.

Il processo analitico dei dati è diviso in più fasi. Una fase preliminare in cui si analizza il contesto in cui i dati verranno utilizzati, i problemi che si vogliono affrontare con i dati; in cui si sceglie quali tipologie di dati si vogliono utilizzare; in cui si decide sull'opportunità di procedere con un'analisi computazionale basata su dati storici, oppure con una predittiva o di affidarsi a strumenti alternativi tradizionali. Una fase di progettazione dell'algoritmo in cui si valuta l'opportunità di scomporre il problema o il quesito oggetto dell'analisi in una serie di sotto-problemi e di calcolare il loro peso e il loro valore rispetto al problema o al quesito generale; di ricorrere alle correlazioni tra i dati⁵¹ o alla somiglianza informatica⁵². In questa fase si tenta di progettare attentamente l'algoritmo in modo tale da inserire correttamente i criteri di funzionamento, così da evitare errori, false regolarità o fattori confondenti nei risultati algoritmici. Una fase finale in cui si leggono, si interpretano i risultati algoritmici, avendo a mente i problemi e il

45. Sulla funzione informativa si v. CAMELLI-GUERRA 1997; MERLONI 2002; MATTARELLA 2006.

46. Sulla funzione statistica si v. GUERRA 2006; GIGLIONI 2005.

47. Per queste tipo di riflessioni si rimanda a FALCONE 2023, pp. 121-125.

48. Sulle caratteristiche dei big data si v. per tutti DE MAURO-GRECO-GRIMALDI-RITALA 2018.

49. L'autonomia della disciplina la si deve a CLEVELAND 2001; PROVOST-FAWCETT 2013.

50. Le discipline coinvolte sono la matematica, la statistica, la scienza dell'informazione, l'informatica e le scienze sociali, in particolar modo nei seguenti sottodomini: basi di dati e visualizzazione dati o business intelligence, intelligenza artificiale o apprendimento automatico.

51. Con le correlazioni statistiche, un insieme di elementi noti contribuiscono a ridurre la nostra incertezza su elementi sconosciuti.

52. Per somiglianza informatica intendiamo un ragionamento per cui due entità simili per caratteristiche o attributi noti spesso sono simili anche per caratteristiche o attributi che sono sconosciuti.

contesto in cui si opera, e si inseriscono all'interno del processo decisionale⁵³.

In un sistema amministrativo come quello italiano, che sta provando a trasformare digitalmente le proprie strutture organizzative e i propri procedimenti, anche per governare le intelligenze artificiali che in futuro verranno utilizzate, la scienza dei dati può diventare un sapere tecnico fondamentale⁵⁴.

5. La *data science* come sapere al servizio delle amministrazioni pubbliche

La *data science* all'interno di strutture organizzative complesse come le amministrazioni pubbliche deve sapersi integrare con i saperi tradizionali, come quello giuridico, quello statistico, quello informatico e quello ingegneristico

Per rendere la prospettiva più concreta, il *data scientist* che lavora nell'amministrazione è una figura professionale che deve essere capace di progettare gli algoritmi, di costruire il set di dati che deve essere elaborato dall'algoritmo, di leggere e interpretare i risultati dell'elaborazione algoritmica, ma deve possedere conoscenze giuridiche, deve conoscere le regole dell'organizzazione e dell'azione amministrativa, il funzionamento delle amministrazioni pubbliche. Inoltre, deve interagire con le altre figure professionali tradizionali presenti nelle amministrazioni. Esso deve progettare l'algoritmo e interpretarne i risultati, veicolando la conoscenza algoritmica nella decisione amministrativa, coadiuvato dagli statistici, e lasciando l'elaborazione e gli aspetti più tecnici agli ingegneri e agli informatici.

Una interazione che dovrebbe trovare luogo in un unico ufficio tecnico, in cui le competenze statistiche, quelle della scienza dei dati, quelle informatiche, quelle di coordinamento e di stimolo alla trasformazione digitale possano costituire il motore della capacità informativa dell'amministrazione di appartenenza.

Il rafforzamento informativo del sistema amministrativo, dunque, passa innanzitutto dalla capacità di rendere la *data science* un sapere

tecnico diffuso nelle amministrazioni pubbliche e un sapere attorno al quale fare ruotare tutti gli altri saperi tecnici relativi alla gestione dei dati, con la consapevolezza che tutti i saperi menzionati sono necessari, ma nessuno di essi può essere sufficiente a garantire un adeguato rafforzamento della capacità informativo delle amministrazioni pubbliche.

Per rendere le amministrazioni pubbliche dei soggetti capaci di amministrare nella rivoluzione dei dati, capaci di valorizzare il proprio patrimonio informativo e di colmare la propria debolezza conoscitiva, gli uffici informativi così come li abbiamo prefigurati non basterebbero, senza una sinergia completa tra questi e i dirigenti e i funzionari delle amministrazioni di appartenenza.

I funzionari e, in particolare, i dirigenti pubblici devono essere capaci di relazionarsi con il *data scientist*, in generale con l'ufficio informativo, devono sapere quali dati raccogliere per comprendere i fenomeni, quali domande porre all'algoritmo per prendere determinate decisioni, devono essere capaci di comprendere i risultati delle elaborazioni e garantire che questi strumenti vengano utilizzati all'interno di un quadro di garanzie a tutela dei diritti protetti dal nostro ordinamento.

Amministrare nella rivoluzione dei dati, in sintesi, non presuppone solo un forte sapere tecnico nelle amministrazioni, ma anche un diverso modo di intendere la managerialità pubblica, la quale deve essere in grado di relazionarsi agevolmente al mondo dei dati e al bagaglio conoscitivo originale che le loro elaborazioni producono⁵⁵.

La *data science* come sapere tecnico e una nuova cultura del dato, diffusa in tutto il sistema amministrativo e in tutti gli uffici amministrativi, capaci di intercettare un fenomeno conoscitivo nuovo, come quello della rivoluzione dei dati, sono i presupposti fondamentali per permettere all'amministrazione di governare la complessità della trasformazione digitale, in particolare in una prospettiva in cui le intelligenze artificiali non saranno strumenti marginale nell'esercizio delle funzioni amministrative.

53. Si v. PROVOST-FAWCETT 2013.

54. In questo senso si riportano le riflessioni di FORTE 2020.

55. Sulla managerialità pubblica si v. PIOGGIA 2007, p. 117 ss.

Riferimenti bibliografici

- S. ACETO DI CAPRIGLIA (2024), *Intelligenza artificiale: una sfida globale tra rischi, prospettive e responsabilità. Le soluzioni assunte dai governi unionale, statunitense e sinico. Uno studio comparato*, in “federalismi.it”, 2024, n. 9
- C. ACOCELLA, A. DI MARTINO (2022), *Il rinnovamento delle competenze nell'amministrazione digitale*, in “Rivista di Digital Politics”, 2022, n. 1-2
- AGID (2023), *Piano triennale per l'informatica nelle pubbliche amministrazioni*, edizione 2024-2026, dicembre 2023
- I. ALBERTI (2022), *La creazione di un sistema informativo unitario pubblico con la Piattaforma digitale nazionale dati*, in “Istituzioni del Federalismo”, 2022, n. 2
- A. AVERARDI, L.F. SAN MAURO (2019), *Ragionare per reclutare: la logica nei (e dei) concorsi pubblici*, Associazione Italiana Professori di Diritto Amministrativo, 2019
- C. BARBATI (2021), *La decisione pubblica al cospetto della complessità: il cambiamento necessario*, in “Diritto pubblico”, 2021, n. 1
- M. BOMBARDELLI (2015), *Semplificazione normativa e complessità del diritto amministrativo*, in “Diritto pubblico”, 2015, n. 3
- G. BUTTARELLI (2022), *La strategia italiana per la tecnologia 5G*, in V. Bontempi (a cura di), “Lo Stato digitale nel Piano nazionale di ripresa e resilienza”, RomaTre-Press, 2022
- F. CAIO (2014), *Lo Stato del digitale. Come l'Italia può recuperare la leadership in Europa*, Marsilio, 2014
- M. CAMMELLI, M.P. GUERRA (a cura di) (1997), *Informazione e funzione amministrativa*, Maggioli, 1997
- E. CARLONI (2024), *Transparency within the artificial administration, principles, paths, perspectives and problems*, in “Italian Journal of Public Law”, 2024, n. 1
- E. CARLONI (2023), *La differenziazione attesa, la differenziazione praticata: spunti su autonomie regionali e digitalizzazione pubblica*, in “Istituzioni del Federalismo”, 2023, n. 2
- E. CARLONI (2019), *Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni*, in “Diritto pubblico”, 2019, n. 2
- G. CARULLO (2023), *Piattaforme digitali e interconnessione informativa nel nuovo Codice dei Contratti Pubblici*, in “federalismi.it”, 2023, n. 19
- G. CARULLO (2020), *Principio di neutralità tecnologica e progettazione dei sistemi informatici della pubblica amministrazione*, in “Cyberspazio e diritto”, 2020, n. 1
- G. CARULLO (2018), *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Giappichelli, 2018
- R. CAVALLO PERIN (2020), *Ragionando come se la digitalizzazione fosse data*, in “Diritto amministrativo”, 2020, n. 2
- R. CAVALLO PERIN, M. LIPARI, G.M. RACCA (a cura di) (2024), *Contratti pubblici e innovazioni nel nuovo Codice. Trasformazioni sostanziali e processuali*, Jovene, 2024
- S. CIVITARESE MATTEUCCI, L. TORCHIA (2016), *La tecnificazione dell'amministrazione*, in Id. (a cura di), “La tecnificazione”, vol. IV, in L. Ferrara, D. Sorace (a cura di), “A 150 anni dall'unificazione amministrativa italiana”, Firenze University Press, 2016

- W.S. CLEVELAND (2001), *Data science: An action plan for expanding the technical areas of the field of statistics*, in "International Statistical Review", vol. 69, 2001, n. 1
- A. CONTALDO (2022), *La piattaforma digitale nazionale dei dati e l'algoritmo: la coesistenza della trasparenza amministrativa con l'efficienza dell'informatizzazione*, in "Lo Stato", 2022, n. 18
- M. DE DONNO, F. DI LASCIO (a cura di) (2022), *Public Authorities and Complexity. An Italian Overview*, Edizioni Scientifiche Italiane, 2022
- A. DE MAURO, M. GRECO, M. GRIMALDI, P. RITALA (2018), *Human resources for Big Data professions: A systematic classification of job roles and required skill sets*, in "Information Processing & Management", vol. 54, 2018, n. 5
- S. DEL GATTO (2022), *Le infrastrutture nella banda ultra larga e il piano per la copertura delle zone a fallimento di mercato*, in V. Bontempi (a cura di), *"Lo Stato digitale nel Piano nazionale di ripresa e resilienza"*, RomaTre-Press, 2022
- M. FALCONE (2023), *Ripensare il potere conoscitivo pubblico tra algoritmi e big data*, Editoriale Scientifica, 2023
- L. FIORENTINO (2013), *I corpi tecnici nelle amministrazioni: problemi attuali*, in "Rivista trimestrale di diritto pubblico", 2013, n. 2
- P. FORTE (2020), *Diritto amministrativo e data science. Appunti di intelligenza amministrativa artificiale (AAI)*, in "P.A. Persona e Amministrazione", 2020, n. 1
- F. GIGLIONI (2005), *Le soluzioni istituzionali alla qualità dell'informazione statistica*, in "Diritto pubblico", 2005, n. 3
- M.P. GUERRA (2006), *L'ordinamento statistico*, in "Dizionario di diritto pubblico", diretto da S. Cassese, Giuffrè, 2006
- C. LOBASCIO (2023), *Tabella riassuntiva dell'evoluzione del diritto europeo dei dati e delle piattaforme*, in "Rivista italiana di informatica e diritto", 2023, n. 2
- B. MARCHETTI (2022), *Amministrazione digitale*, in "Enciclopedia del Diritto. Funzioni amministrative", Giuffrè, vol. 3, 2022
- B. MARCHETTI, L. PARONA (2022), *La regolazione dell'intelligenza artificiale: Stati Uniti e Unione europea alla ricerca di un possibile equilibrio*, in "DPCE online", 2022, n. 1
- B.G. MATTARELLA (2006), *Informazione amministrativa*, in "Dizionario di diritto pubblico", Giuffrè, 2006
- G. MELIS (2019), *Culture dei «tecnici» e amministrazione nell'Italia di ieri e di oggi*, in "Rivista giuridica del Mezzogiorno", 2019, n. 2
- G. MELIS (2013), *La fuga dall'amministrazione. Ascesa e declino dei tecnici nell'amministrazione dell'Italia unita*, in "Rivista trimestrale di diritto pubblico", 2013, n. 2
- F. MERLONI (2022), *Il d.lgs. n. 165 del 2001 e l'organizzazione delle competenze professionali dei funzionari pubblici*, in "Diritto amministrativo", 2022, n. 2
- F. MERLONI (2018), *Costituzione repubblicana, riforme amministrative e riforme del sistema amministrativo*, in "Diritto Pubblico", 2018, n. 1
- F. MERLONI (2008), *Coordinamento e governo dei dati nel pluralismo amministrativo*, in B. Ponti (a cura di), "Il regime dei dati pubblici", Maggioli, 2008
- F. MERLONI (a cura di) (2002), *L'informazione delle pubbliche amministrazioni*, Maggioli, 2002
- A. MOLITERNI (2017), *Semplificazione amministrativa e tutela degli interessi sensibili: alla ricerca di un equilibrio*, in "Diritto amministrativo", 2017, n. 4

- E. MONTAGNANI (2022), *Le pubbliche amministrazioni nell'era delle tecnologie "cloud" ed "edge computing" tra opportunità e rischi: il Piano Nazionale di Ripresa e Resilienza e le comunità digitali*, in "Rivista italiana di informatica e diritto", 2022, n. 1
- A. PIOGGIA (2007), *La managerialità nella gestione amministrativa*, in F. Merloni, A. Pioggia, R. Segatori, (a cura di), "L'amministrazione sta cambiando? Una verifica dell'effettività dell'innovazione nella pubblica amministrazione", Giuffrè, 2007
- A. PIOGGIA (2005), *L'organizzazione e le nuove tecnologie*, in F. Merloni, "Introduzione all'e-government. Pubbliche amministrazioni e società dell'informazione", Giappichelli, 2005
- P. PIRAS (2021), *Semplificazioni e buon andamento della Pubblica amministrazione. Tra Scilla e Cariddi: rispettare la complessità superando le complicazioni*, in "DPCE online", 2021, n. 2
- P. PIRAS (2020), *Il tortuoso cammino verso un'amministrazione nativa digitale*, in "Diritto dell'informazione e dell'informatica", 2020, n. 1
- B. PONTI (2023), *Tre scenari di digitalizzazione amministrativa "complessa": dalla interoperabilità predicata alla standardizzazione praticata*, in "Istituzioni del Federalismo", 2023, n. 3
- B. PONTI (2008), *Coordinamento e governo dei dati nel pluralismo amministrativo*, in "Informatica e diritto", 2008, n. 1-2
- F. PROVOST, T. FAWCETT (2013), *Data Science and its Relationship to Big Data and Data-Driven Decision Making*, in "Big Data", vol. 1, 2013, n. 1
- G. ROSSI (2021), *Principi di diritto amministrativo*, Giappichelli, 2021
- L. SALTARI (2019), *Che resta delle strutture tecniche nell'amministrazione italiana?*, in "Rivista trimestrale di diritto pubblico", 2019, n. 1
- A. SANDULLI (2021), *Pubblico e privato nelle infrastrutture digitali nazionali strategiche*, in "Rivista trimestrale di diritto pubblico", 2021, n. 2
- G. SGUEO (2022), *Reclutamento e formazione del personale*, in V. Bontempi (a cura di), "Lo Stato digitale nel Piano nazionale di ripresa e resilienza", RomaTre-Press, 2022
- S. STACCA (2019), *La selezione del personale pubblico al tempo delle tecnologie digitali*, Associazione Italiana Professori di Diritto Amministrativo, 2019
- A. ZUCARO (2019), *La crisi dei Corpi Tecnici della PA nel quadro della crisi delle politiche pubbliche*, in "Rivista giuridica del Mezzogiorno", 2019, n. 2

Studi e ricerche

Sistemi e applicazioni

Note e discussioni

Osservatori



PILAR MARTÍN RÍOS

Predictive algorithms and criminal justice: expectations, challenges and a particular view of the Spanish VioGén system

The irruption in the field of the Administration of Justice of instruments linked to Artificial Intelligence and to the algorithms on which it is frequently based, is a well-known reality. In addressing this issue, some problems will inevitably need to be resolved, relating to access to justice, transparency or the impact of the digital divide. In this study, we will focus on the examination of AI in the Administration of Justice in general and, specifically, on its influence on criminal proceedings. Within this framework, we will also examine the emergence of the use of systems that, while employing algorithms, do not meet the criteria that allow them to be classified as AI. We will focus on the Spanish case, using the VioGén system as a paradigmatic example, although it is unavoidable to refer to the overall situation, given the global dimension of the analyzed phenomenon.

Criminal process – Artificial Intelligence – Predictive justice – Precautionary measures – VioGén

Algoritmi predittivi e giustizia penale: aspettative, sfide e una visione particolare del sistema spagnolo VioGén

L'irruzione nel campo dell'amministrazione della giustizia di strumenti legati all'intelligenza artificiale e agli algoritmi su cui spesso si basa è una realtà ben nota. Nell'affrontare questo tema, sarà inevitabile risolvere alcuni problemi legati all'accesso alla giustizia, alla trasparenza o all'impatto del digital divide. In questo studio ci concentreremo sull'esame dell'IA nell'amministrazione della giustizia in generale e, nello specifico, sulla sua influenza sui procedimenti penali. In questo contesto, esamineremo anche l'emergere dell'uso di sistemi che, pur impiegando algoritmi, non soddisfano i requisiti che consentono di classificarli come IA. Ci concentreremo sul caso spagnolo, utilizzando il sistema VioGén come esempio paradigmatico, anche se è inevitabile fare riferimento alla situazione generale, data la dimensione globale del fenomeno analizzato.

Processo penale – Intelligenza Artificiale – Giustizia predittiva – Misure cautelari – VioGén

The Author is Associate Professor of Procedural Law at the University of Seville (Spain)

Work carried out within the project *Transición digital de la Justicia*. Ref.TED2021-130078B-I00 (Spanish Ministry of Science and Innovation)

SUMMARY: 1. Methodological premises. – 2. Preliminary considerations: the emergence of Artificial Intelligence (AI) in the Administration of Justice. – 3. The case for Criminal Justice. – 3.1. *General considerations.* – 3.2. *Possible virtualities of police use of AI in criminal cases: detection, deduction and prediction.* – 3.3. *AI and judicial activity: algorithms and the right of defense.* – 4. Particularizing the study: the algorithmization of the adoption of precautionary measures. – 4.1. *Initial considerations.* – 4.2. *The Spanish case: VioGén.* – 5. Discussion. – 6. Conclusions.

1. Methodological premises

The application of Artificial Intelligence (AI) and the use of algorithms in the Administration of Justice – particularly in the criminal field – has proven to be an invaluable tool in case management and decision making. In our paper we will go from the general to the particular, starting with the analysis of such techniques and tools in the Administration of Justice in general, to then descend to the criminal justice level and, within it, to do the same in relation to the precautionary protection. Within the latter, we will use an empirical-inductive approach to analyze the VioGén system by examining a Spanish case.

For this work we have used the logical method, both analytical and deductive¹. We have also sought a critical and proactive approach, being the proposal of solutions our main pretension.

In terms of methodological techniques, jurisprudential analysis plays a crucial role in our study, without neglecting the due examination of numerous legal texts (Spanish Constitution, organic and ordinary laws, international treaties and European regulations), as well as abundant recent scientific doctrine.

2. Preliminary considerations: the emergence of Artificial Intelligence (AI) in the Administration of Justice

We cannot ignore the fact that modern justice tends to be, in a universal way, a “data-oriented” justice², so the competent judicial authorities will have to handle a high volume of data in their decision-making process. Undoubtedly, the availability of large amounts of information will require AI-based methods to manage it³.

Although the implementation of technological tools facilitates the resolution of many of the problems that hinder the effectiveness of justice, it cannot be ignored that, at the same time, it has become the origin of other different ones. Precisely for this reason, having an adequate and sufficient regulation of its application and development is, more than ever, an unavoidable requirement.

Both the transparency and efficiency of the Administration of Justice would be enhanced by an adequate transition from analogue to digital. However, on occasions there has been a certain haste in the implementation of instruments, channels or techniques linked to new technologies, without

1. MARTÍNEZ MONTENEGRO 2023.

2. As stated by the [Spanish Ministry of Justice](#). Also of particular interest is CTEAJE 2022.

3. In Spain, for example, different regulatory initiatives have been developed in this regard. The project *Artificial Intelligence for the Efficiency of Justice* is a good illustration of this. Its aim is to adapt AI to advanced judicial analytics, improve the management and knowledge of data to apply it to processes, guide legislative policies through a better understanding of the impact of data associated with legal regulations, facilitate the automatic translation of rules and resolutions into the co-official languages of the State and implement a comprehensive open data policy in the Administration of Justice.

the accompaniment, in addition, of adequate training or investment of material or human resources. These objective limitations increase the reluctance of some legal operators in the face of the technification of Justice, which constitutes one of the main obstacles to its proper development.

Moreover, while it is still necessary to adapt the classic structures of law to the new demands arising from the technological revolution, it should not go to the extreme of thinking that it would be necessary to reformulate the General Theory of Law to find a specific legal fit for this new reality. In short, it is a matter of trying to anticipate this new, much more complex reality at the regulatory level, so that it is the law that imposes the guidelines on AI, and not vice versa⁴.

It is an undeniable necessity to subject AI to legal standards that guarantee that its operation will respect the rights of others. The EU's regulatory efforts are heading in precisely this direction. In the European context, the 2019-2023 Action Plan on European e-Justice contemplates as one of its fundamental pieces the progress in the application of AI in the field of Justice, defining in a more appropriate way the digital implications in this area and specifying the role of AI in the analysis of judicial decisions.

For its part, the European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe, in the conviction that AI can contribute to improving the efficiency and quality of the work of the courts, adopted in 2019 the first European Ethical Charter on the use of AI systems in judicial administrations. To this end, it sets out some basic principles: respect for human rights, quality and security in the analysis and automated procedure of judicial decisions, transparency in the methodology used during judicial decision-making and the promotion of control exercised by users, who must be informed of their rights with respect to the

solutions proposed through means based on AI. These will therefore be the premises from which we will start our study, analyzing to what extent the current development/implementation of AI in our environment respects these elementary premises.

In December 2023, the European Parliament and the Council of the EU – in response to a request from the European Commission in 2021 along the same lines⁵ – reached a political agreement on the AI Act. Final text was published on 12 July 2024⁶. The AI Act shall apply from 2 August 2026, with some exceptions. It responds to a fundamental objective: to ensure that the AI systems used in the EU are safe and respect citizens' rights. In this line, a "risk-based" approach is followed: the higher the risk, the stricter the rules⁷. The EU AI Act is the first comprehensive legal framework on AI worldwide, although China (*General AI Regulatory Law*) and the USA (*Executive Order Safe, Secure and Trustworthy Development and use of AI*) have approved AI regulations in recent times (2023).

3. The case for Criminal Justice

3.1. General considerations

With regard, in particular, to its use in the field of Criminal Justice, as a part of a broader trend characterized by the increased use of forensic science and scientific procedures within it – in the belief that they can provide the judge with more objective, safe and controllable elements⁸ –, the irruption of the AI has placed us in a scenario of uncertainty. Even if one wants to trust in the potential it offers, it is inevitable to be suspicious of what is still an unfathomable terrain.

Algorithms can have various functionalities in the context of criminal proceedings. Alongside a hypothetical – and unrealistic, in our opinion – gradual replacement of the judge by a "robot judge", there are more feasible uses which may be of some

4. RODRÍGUEZ LAINZ 2023.

5. *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021) 206)*.

6. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

7. As stated in the EU AI Act.

8. BRIGHI 2016; MOSCARINI 2015.

relevance. Thus, for example, it facilitates the analysis of large amounts of data that may have evidentiary value in a process, and it does so quickly and efficiently.

Not even the profusion of rigorous scientific studies on this subject⁹ manages to dispel all the doubts raised by the assumption of algorithm-based tools and resources in this field, that has even motivated the existence of an “algorithmic criminal justice” to be considered¹⁰.

The question must be analyzed in the light of the necessary respect for the protection of procedural rights and guarantees and the principle of “electronic judicial security” in all its dimensions: authenticity, confidentiality, integrity, availability, traceability and preservation (art. 53.2 [Spanish] Law 18/2011 of July 5, 2011, regulating the use of information and communication technologies in the Administration of Justice).

From a more particular perspective, we could not argue that AI can collaborate with the defense in planning and developing their own strategies in the process. In fact, more and more law firms have various AI tools that allow, through massive data processing, both the calculation of the chances of success of a given claim and the identification of patterns in judging activity. Although these are utilities that are not yet widespread in Spain, in the United States AI is used to challenge juries and judges, as well as to question the impartiality of witnesses.

On the other hand, it should be noted that AI could even favour the interaction of vulnerable groups with the justice system. Undoubtedly, various technologies that use AI would serve to improve the accessibility to the process for those

who have a physical or mental disability, or for those who do not know the language used in the proceedings. In this way, they could make the documents included in the case more accessible (through their reading or automatic translation, if necessary), facilitate access to judicial information and, at the same time, make communication with the parties possible (or simplify, as the case may be). To sum up, it would be possible to provide technological support that, compensating for its limitations, helps those who need it to be and act in the process in the best possible way.

AI is presented, in addition to the above, as a useful tool to support victims of crime. In particular, AI-powered chatbots and virtual assistants offer information and support in cases of gender-based violence, especially in cases where women – having normalized certain behaviors over time – do not identify with the role of victims. Both in these cases and in those in which there is a paralyzing fear of expressing the situations they suffer, the anonymity and support guaranteed by this type of chatbot make them allies of notable importance.

Along with these well-known functionalities, there are other applications that are based on AI technology that are not as widely used. This is the case of biometric programs that proceed to voice recognition through AI techniques, which have been used – again, in victimization linked to gender violence – to detect traits in the victim that allow the identification of criminal behaviors that have been committed against them¹¹. Together with these uses, we will examine how it can contribute to the development of the criminal procedure itself, and how it can compromise its basic principles.

9. MARTÍN DÍZ 2021; NIEVA FENOLL 2018; VALLESPÍN PÉREZ 2023.

10. HUQ 2019; BARONA VILAR 2021.

11. Due to its relevance, it is interesting to bring up the program led by the UNODC-INEGI Center of Excellence, in Mexico City, which uses AI to analyze the calls received by 911 and detect, in them, the presence of gender-based violence. With the technique used, based on natural language processing, the aim is to identify emotions in the voice of those women who, having contacted 911 for other types of issues, could be experiencing an episode of gender violence. In Andalusia (Spain), on the other hand, with the collaboration of the Andalusian Women's Institute, the project “Certainty of the voice” is being developed, which seeks to design a common voice pattern through the calls made by women to the health emergency number (061). Even if they have not claimed to be victims of abuse at any time, AI is used to analyze their words, the expressions used, the intonation, the rhythm, the pauses, the repetitions and even the silences that can be observed in those calls. In short, even the smallest detail that may reveal an emotion that is associated with suffering from a situation of victimization is taken care of.

3.2. Possible virtualities of police use of AI in criminal cases: detection, deduction and prediction

The involvement of AI in the criminal justice field cannot be examined without reference to its use by police forces. In our view, three possible virtualities can be identified in the use of AI in policing: detection, deduction and prediction. It is through this prism – the examination of AI in these three facets, which we believe can be identified – that we will approach this question.

As regards the first of these, AI contributes to the “detection” of certain circumstances. In particular, a system has been developed in Spain that allows the identification of false reports. Under the name “VeriPol”, it is a system that, using natural language processing methods and a mathematical model, evaluates the probability of a complaint being false. It also makes it possible to identify patterns of behaviour, in such a way that it is able to determine which are the singularities that most distinguish false reports. In short, the aim is to elucidate the veracity of statements made by possible victims of crime. Apart from the fact that it does not require any information from the user, and is fully automatic, empirical experiments show that it is over 90% accurate, while expert police officers are over 75% accurate¹².

In 2014, a team of researchers from a Spanish and an Italian university developed this pioneering tool, which is based on examining the language used in a report to indicate the likelihood of it being true. It was created for cases of theft and robbery with violence and intimidation, due to the fact that it is in these areas where an increase in the number of simulated crimes has been detected in recent years.

From this analysis it can be concluded that true and false reports differ mainly in three main aspects: *modus operandi* of the aggression, morphosyntax of the report and amount of detail¹³.

Continuing with the detection work, AI-based tools also help to detect the presence of certain individuals in particular places. This is particularly useful in the course of a criminal investigation and also at the police level, to allow for a massive policing. In this respect, AI makes it possible to analyze huge amounts of data, e.g., from video and audio recordings. It undoubtedly facilitates criminal investigation to a very considerable degree¹⁴.

We find, in this respect, AI-based technology that enables facial recognition. Even though this and other biometric technologies are particularly risky, as highlighted by Murakami¹⁵, its use is widespread in several areas¹⁶. It is significant that the proposed European Regulation referred to above, which is the result of the agreement reached in 2023, now contemplates something that it did not initially do: the possibility of remote, real-time biometric identification in public spaces, provided that it is carried out by law enforcement authorities and subject to certain safeguards¹⁷.

In addition to these uses of mere detection or identification, AI facilitates, in a deductive way, the discovery of the alleged perpetrators of a criminal act. It provides information that is relevant to such deductive activity and does so, moreover, by providing standardized data based guidance for case handlers to collect, examine and verify evidences¹⁸. The RACR system and the Patternizr tool, both used in the United States, are also highly significant¹⁹. In both cases, patterns are identified and, by establishing relationships between them, it is easier to determine the presumed perpetrators.

12. According to data from the [Spanish Ministry of the Interior](#).

13. ALONSO 2021.

14. GARCÍA SÁNCHEZ 2022.

15. MURAKAMI WOOD 2006.

16. The control of transport and airports, in particular, although it is even being implemented in companies to facilitate payments.

17. This will only be possible for the commission of certain crimes, the prevention of real threats and the search for people suspected of the most serious crimes. On the other hand, indiscriminate tracking of facial images taken from the internet or CCTV is not allowed.

18. CUI 2019.

19. ALONSO 2021.

Besides from that, in the field of crime prevention, the use of AI by the police is a reality that is growing exponentially, in the framework of what is known as predictive policing. The predictive tools (as CAS, Crime Anticipation System) make it possible to identify places where crime is most likely to be committed (the so-called crime heat maps, where the “hot spots” can be recognised). AI also allows these maps to be dynamic, real-time maps²⁰.

In other words, it will be sufficient to have data enough for the corresponding algorithm to yield information about the probability of a behaviour being carried out, as a mere statistical reflection, bearing in mind that the usefulness of predictive techniques will vary according to the crime in question²¹. Knowing this data undoubtedly helps to make patrolling more effective and results in a better distribution and use of material and human resources.

Regardless of the aforementioned, from a predictive point of view, there is a growing use of algorithms for the calculation of probabilities of different kinds (and not only in the field of policing, as we shall see). In general terms, we can define predictive analytics systems as the application of machine learning or deep learning capable of extracting patterns from historical data to predict future events or behaviours, giving a numerical value or score to the probability of a particular event happening, and suggesting actions to obtain more optimal results²².

This would be the case, for example, with its possible use when determining the possibility of recidivism of an offender and, consequently, as an instrument for carrying out a prognosis for social reintegration and as a tool for assessing victim risk²³. In our opinion, it should be, in any case, a support for the work of the judiciary and not a usurpation of it, since it takes on a different dimen-

sion when it ceases to be “just another instrument” and becomes the core of the judicial decision, as we will have occasion to explain. However, courts heavily weigh these models in their decisions²⁴. COMPAS, in the United States, RISC, in Netherlands, or PSA (Public Safety Assessments), in the United Kingdom, are just a few examples.

The greater risk arises, in our view, when it comes to quantifying the probability that a given person will commit a crime, as in the case of the UK algorithm HART (Harm Assessment Risk Tool). It is even done to determine the possible serial criminal action of a person²⁵, through crime linking systems, such as Keycrime or Precobs software. Undoubtedly, the latter use presents greater problems in terms of acceptance. Precisely because of its importance, it will be the one that occupies our attention in the following sections.

3.3. AI and judicial activity: algorithms and the right of defense

In the following pages, we will analyse how the shift towards a justice system in which the algorithmic function plays a considerable role could affect the due respect for the right of defense. It is not a theoretical exercise, carried out on a hypothetical and future plane. Algorithms are already being used in the Administration of Justice, although they still do so on a small scale, in very specific areas, and have not even come close to reaching all the development of which they are capable.

In this regard, we must bear in mind the words of Paulesu²⁶, who wonders how the use of AI can be combined with respect for the table of values (constitutional and supranational) that characterises the fair process (equality of arms, personal freedom, right to defense, presumption of innocence, contradiction and impartiality of the judge). This is, of course, a considerable legal challenge, and must

20. CUSTERS 2022.

21. CEPEJ 2019 states that there are crimes that are not so regular in nature, or that are simply characterised by the fact that their effects are produced in different locations. In these cases, the predictions that can be made will be less relevant.

22. GARCÍA 2023.

23. The VioGén system is a clear example of this.

24. CUSTERS 2022.

25. BASILE 2019.

26. PAULESU 2023.

also be our starting point, the prism from which we approach our research: the needed balance between AI and the respect for these rights.

Let us start from the premise that all parties to the proceedings, including the accusers, must – as a manifestation of the right to obtain effective judicial protection – be guaranteed the exercise of their rights of defense. However, the limitations that may occur in the framework in which we now operate are perhaps most evident with regard to the subjects involved in a process. It is obvious that they must have an effective possibility of defending themselves, and this will depend, in practice, on respect for certain guarantees in the process.

Equality, which, as an inalienable principle of the process, must be verified throughout its development, is one of the main victims of an algorithmic criminal justice model. The so-called “digital divide” is particularly important in this area. It is undeniable that the imbalance of economic resources will translate into unequal access to certain AI systems, which could have a decisive impact on the future of a process. This difference will be particularly significant in civil proceedings, by virtue of the interplay of the dispositive principle. In criminal cases, it is expected that these techniques and remedies will be applied, *ex officio*, by the judge. This gap can also be seen in the unequal digital training of legal operators, which will lead to a deficient application of available AI resources.

For instance, reflect on the complexity of defending oneself against evidence and allegations that are primarily based on algorithmic systems, which are inaccessible to those affected by their procedural consequences. Furthermore, consider how our conception of the right to defense would shift if, in scenarios where the principle of opportunity is applied, negotiations over a potential conviction were conducted between a robot prosecutor and a robot defense attorney²⁷.

In order to ensure that the difference in status between the parties does not result in unequal access to justice and an impediment to the effective exercise of the rights of defense, it may be appropriate to adapt the benefits included in the benefit of legal aid to the new times and extend them to

more current demands, such as the use of the latest AI technologies and access to techniques for the mass processing of legal aid.

This is not the only area in which equality could be compromised. AI systems can present biases – as is well-known from the *Loomis case*²⁸ –, which will be those of the individuals who configure the algorithms on which they are based. The prejudices and inequalities that are at its base will be predictably reflected in its outcome. For that reason, recital 71 of Regulation (EU) 2016/679 (Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) calls for the application of a principle of algorithmic non-discrimination, to avoid what is known as GIGO (garbage in, garbage out), that is, that the algorithm is built on data that is, in origin, discriminatory.

In addition, taking into account the difficulties inherent in any process of purging responsibilities that could result from the inadequate functioning of algorithms, it will be particularly complex to demand accountability in the event that a situation of injustice does occur.

Progressively, society is becoming aware that the exchange of data that takes place between large companies to draw profiles of potential customers must be subject to control and transparency. In the US, for example, the recent Algorithmic Accountability Act obliges large companies – provided that certain requirements are met – to audit their algorithms.

It seems understandable that similar clarity should be required when it comes to the creation of profiles or patterns that serve the fulfilment of police functions of crime prevention and detection. In the same way, value judgments must be made about the probability of recidivism of a subject. In any case, it is advisable to insist on the importance of preventing them from being based on *ab initio* discriminating algorithms. Otherwise, there would be a perpetuation of certain inequalities and prejudices that clearly need to be eradicated²⁹.

Transparency, in the end, is a basic condition for the proper exercise of the rights of defense. While this necessity is evident in any judicial pro-

27. FERNÁNDEZ GALARRETA 2021.

28. On the *Ewert case*, similar to the *Loomis case*, see GIACOMELLI 2019; VALLESPÍN PÉREZ 2022.

29. VILLEGAS DELGADO 2023.

cess, where every decision is documented and justified through “traditional” means, it becomes even more relevant when procedures or decision-making processes are based on the application of algorithms.

The problem lies not only in the scientific-technical complexity of the arguments that could be used to justify decisions based on mathematical formulas – the understanding of which will only be available to those with specific training in this regard³⁰ – but also in the publicity that is made of the technology used as the basis for them. An example of this is the software used, which should always be provided by public bodies and purchased in accordance with transparent tender conditions, subject to all the necessary control guarantees. It is certainly not a matter in which private initiative should be given an unrestricted entry, at the risk that interests other than the general ones will inspire the development of the algorithms that, in the end, will sustain decisions of enormous importance. It seems understandable that any judicial decision taken on the basis of an algorithm is subject to suspicion.

It is evident that nobody could attack with expectations of success what does not properly know. For this reason, basing decisions that have a certain relevance for the individual – as important as the adoption of a personal precautionary measure, for example, could be – on “black box” systems does not exactly contribute to diluting the reservations that exist in this regard³¹.

While it is true that the mental mechanisms guiding a judge’s decision-making are not fully understood, it is also true that this process is supported by at least two safeguards: recusal in cases where the judge’s impartiality is questioned, and the requirement to provide reasoned judgments, which are subject to review through appeals. None of this is possible if we ignore the major premise: who, according to what criteria, developed the algorithms on which the decision is based.

But we must also consider a very different point of view: AI requires huge amounts of data for its operation, which feed the different algorithms on which a given system is based. On the

basis that the confidentiality of the information in the proceedings is a requirement inherent in the same right of defense, it is necessary to draw clear limits that prevent sensitive information of the accused from nourishing this system, even though it could be useful for making predictions about their conduct.

Restrictions on publicity and transparency bring with them another important limitation, which now relates to the adversarial principle. It seems logical to deduce, from what has been stated, the impossibility of contradicting or refuting the results produced by an algorithm, result of a mathematical operation that is elusive and difficult to control. The possibility for the passive party to the proceedings to know and refute the evidence used against him will be clearly limited in such circumstances.

That the technology used at any stage of the procedure is known, accessible and verifiable is a requirement for its questionability. On the contrary, it leads us to a state of uncritical acceptance of the dictates of AI that will lead, in addition, to a situation of absolute defenselessness, to a true tyranny of the algorithm.

In our opinion, the use of algorithms designed ad hoc can facilitate – but not replace, since this is a barrier that we consider insurmountable – the work of the judge. It would be, in other words, an additional tool to obtain the precise information to decide in conscience.

In any case, it is essential that law enforcement and judicial authorities are always able to separate themselves from this interpretation, avoiding the potentially serious consequences that derive from an absolute adherence to the algorithm. As highlighted in the European Parliament Resolution 2020/2016 on artificial intelligence in criminal law and its use by law enforcement and judicial authorities in criminal matters of 6 October 2021, placing excessive reliance on the apparently objective and scientific nature of AI tools, which ignores the possibility that their results may be incorrect, incomplete, irrelevant or discriminatory, brings with it not inconsiderable risks.

30. ŽIVKOVIĆ–DUCATO 2023.

31. COTINO HUESO 2017; DONATI 2020; GONZÁLEZ ÁLVAREZ–SANTOS HERMOSO–CAMACHO COLLADOS 2020; PÉREZ ESTRADA 2019; SAN MIGUEL CASO 2021; SIMÓN CASTELLANO 2021.

In this sense, we endorse, point by point, the following reflection of Judge Del Moral: «never, at least in the field of criminal justice (another thing is the civil sphere, in which the dispositive principle opens other doors), should we dispense with the primacy and protagonism of the human factor, of the judge who makes the decision. There are variables that a machine, AI, cannot provide. Judicial decisions emanating from a robot may be accurate. But justice is not the same as accuracy. We only approach Justice (without achieving it, but without renouncing that aspiration) through human decisions. That brings with it the potential for errors. But a robotic justice, entrusted to AI, would constitute a justice, perhaps without errors, but dehumanized (in the pejorative sense of the word). In short, it would not be justice»³².

Since, in any case, the final decision will have to be taken by the judge – in that conception that we defend of the algorithm as a support, not as a substitute – it would be expected, in the scenario we describe, that it would be the judicial reasoning that would be discussed by the person affected by the measure, and not the operation of the computer program used, which would require a technical-scientific knowledge superior to that of the average citizen. The problem will arise if this reasoning is limited to being a reference to the result offered by the algorithm, automatically accepted and assumed as its own. In order to prevent the use of any algorithmic support system from infringing the rights of the defense, it will be necessary for it to be accompanied by a threefold requirement: human control of the operation, the possibility of departing from the suggested result and an exhaustive justification of why one way or the other is being taken. Any mere statement of reasons by reference, in view of the risks involved, should be expressly prohibited³³.

4. Particularizing the study: the algorithmization of the adoption of precautionary measures

4.1. Initial considerations

Without leaving the field of criminal justice, we will focus our attention on a very sensitive issue: making a prediction of a person's criminal tendency on the basis of mathematical formulas. Although judicial decision-making linked to the consideration of possible future behaviour is not new in our criminal prosecution³⁴, it would be different if AI techniques were used to make prognoses of dangerousness in an attempt to justify the adoption of pre-criminal measures or even the classification of citizens according to their criminal propensity. The application of these expert systems for predictive purposes in the judicial determination process is encompassed within what is known as Judicial Artificial Intelligence (JIA), whose subtype, Risk Assessment Artificial Intelligence (RVAI), is particularly noteworthy³⁵.

It is undeniable that the criminal justice system sometimes resorts to predictive judgements. Both in the adoption of security measures in criminal proceedings and in the application of social reintegration prognoses in the execution phase of sentences, value judgements are made.

Whether or not an algorithmic program is used for this purpose, there is no doubt that the application of a security measure is always caused by the realization of a previous forecast. In this case, its adoption is not based on the idea of guilt, but takes into account, among other aspects, the dangerousness of the subject, which must be proven within the process and may be subject to contradiction.

But what is the basis of such a judgment of dangerousness? Sometimes it is related to the very pathological states that led to the assessment of non-imputability or semi-imputability; in others, it follows from the very nature of the fact. In any case, and this is the most relevant thing, these are

32. DEL MORAL 2023.

33. In the same way, see the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (Brussels 8 April 2019 COM(2019) 168), *Building Trust in Human-Centric Artificial Intelligence* and the *Guidelines for Trusted AI developed by the High Level Expert Group on AI*.

34. QUATTROCOLO 2020.

35. GARCÍA 2023.

objectively appreciable circumstances, since the security measures are based on the criminal dangerousness of the subject on whom they are imposed, externalized in the commission of an act foreseen as a crime.

The prognosis of future behavior that reveals the probability of committing new crimes is made to depend, apart from the nature and circumstances of the act, on “the personal circumstances of the subject”, which could complicate this interpretation. Despite this, an examination of practice leads us to conclude that even in these cases, objective or “objectifiable” factual notes, such as the mental state or the medical-psychiatric history of the accused, are considered to be “personal circumstances”. In other words, with a view to the imposition of a security measure, psychological examinations are not carried out to assess a possible inclination to crime. Nor is there the use of algorithmic programs to determine it.

As regards what happens at the stage of execution of the sentence imposed, it cannot be denied that reports are drawn up which do identify a certain tendency to commit offences and which serve as the basis for the preparation of a prognosis of recidivism. In practice, this type of data is used to make a prognosis for the social reintegration of convicted persons and to decide whether they should be entitled to prison benefits or access to the third degree or parole. However, there are two points to bear in mind regarding this possibility: firstly, these reports are prepared by experts, integrated into multidisciplinary teams with extensive training and experience. Therefore, mathematical programs that rely on algorithms are not used. Secondly, these are convicted persons, who no longer enjoy the presumption of innocence, so there would be no qualms about alluding to their dangerousness or risk of recidivism.

Having established the above, we must address what happens in another particular area of criminal prosecution: precautionary protection. Predictive justice, which is based on the application of algorithms, finds – at least from a theoretical point of view – a particularly favourable field in the possible adoption of precautionary measures. Such adoption is, in fact, based on the making of judgments of probability. In criminal proceedings,

in particular, the imposition of pre-trial detention – configured, as we know, as the most restrictive personal precautionary measure – depends on the assessment of at least one of the so-called “three risks”: flight, repeat offence or destruction, alteration or concealment of evidence. In that regard, it must not be forgotten that the assessment of a risk really requires the drawing up of a prognosis for a specific person.

It is clear that, when adopting precautionary measures, the risk of recidivism and re-victimization is taken into account. All this, translated into the language we are now using, is intimately linked to that dangerousness to which we have already referred, so it is necessary to ask ourselves on what basis the judge’s judgment is based on this possibility of criminal repetition that then leads him to impose a precautionary measure. Of course, it does so on the basis of objective data, derived from the very nature and circumstances of the act allegedly committed. No objection can be raised in that regard.

Greater problems would arise, however, if, along with this type of information, the judge were to assess another series of characteristics linked, as we said, to the personality or character of the subject in question, from which it could be deduced – that is what is really risky (above all, because the presumption of innocence still operates, at this moment, in full force) – a “tendency to crime”.

In other words, we would only have to accept that a precautionary measure is due to the assessment of the risk of recidivism when this could be objectively founded, as is the case with the prognosis of danger that precedes the imposition of a security measure, as has been said. If its adoption were made in view of the personality of the person (by analysing, for example, the websites visited, the media consulted, the blogs participated in, the tweets published or, in general, the opinions expressed on the Internet), we consider that the presumption of innocence of the person who has to bear it would be compromised. We would also be entering the dangerous terrain of offender-based criminal law. As Paulesu points up³⁶, it is necessary to avoid “juxtaposing the assessment of personality and the assessment of responsibility”.

And, in assessing that risk of recidivism, would it be admissible to obtain that information from

36. PAULESU 2023.

some algorithmic system? Leaving aside the undeniable difficulty implicit in any effort to anticipate human behavior, we must analyze whether making precautionary measures dependent on predictions of algorithmic origin would help to facilitate their application or, on the contrary, would pose an additional problem. There are those who argue, in this regard, that this prognosis is more easily admissible when it is made by a person (even if it is made on the basis of vague and difficult to verify criteria), and more criticizable when it is made by a machine³⁷.

It is not hidden from us that, in fact, the use of algorithmic predictive systems aimed at the application of a precautionary measure is a reality in various legal systems. However, difficulties are observed both in the way these systems are designed and in the way they are developed: first of all, because trying to determine the existence of such a tendency, before a conviction is handed down, implies, as we said, a clear compromise of the right to the presumption of innocence; secondly, because in these cases it is essential to know what kind of information will be used to make such a value judgment. Regardless of the general criticisms about the obscure functioning of algorithms (and the recurrent mention of the *black box system*)³⁸, where could the algorithmic programs used obtain information³⁹ on a hypothetical tendency to commit a crime? It should be borne in mind that, in criminal proceedings – at least in Spain⁴⁰ – judicial expert opinions are only carried out to determine the imputability/non-imputability of the accused.

4.2. The Spanish case: VioGén

In Spain, the fight against gender-based violence shows remarkable singularities in the matter at hand. Although the assessment of any “inclination to crime” (which today may be based on psychological examinations and, tomorrow, may consist of genetic or epigenetic analyses), should not be included in the declaratory phase of the criminal process, where the presumption of innocence still applies, it is true that in the field of gender-based violence – surely due to the frequent revictimization that accompanies this phenomenon and the need to put a stop to it – the Comprehensive Forensic Assessment Units (UVFI)⁴¹ make recidivism prognoses of the aggressor taking into account, among other data, his personality. This prediction is made, of course, in a “traditional” way, without resorting to AI systems, through the joint work of professionals in medicine, psychology and forensic social work. The fact that the psychological profile of the alleged aggressor is drawn up by expert multidisciplinary teams can be accepted as necessary in the fight against such a major problem.

However, we are more concerned about the fact that, in order to make these probability judgments to which we alluded, ad hoc computer programs are used. For years, in order to prevent gender-based violence, State security forces have resorted to the “police risk assessment” protocol (known as VPR), which is the main core of the VioGén system⁴². It is the police who reflect in their report the percentage of risk of revictimization, as estimated by the VioGén system. This interpretation is made automatically, based on the algorithmic reading of the

37. CONTISSA–LASAGNI–SARTOR 2019.

38. In our view, the lack of knowledge about the functioning of algorithmic activity can give rise to two extreme and opposing positions: the uncritical acceptance of the conclusions reached, as we have seen, or the general distrust of the answers offered. In this regard, as some authors point out (CONTISSA–LASAGNI–SARTOR 2019), it is necessary to move from an approach based on “data fundamentalism” to one based on informed trust.

39. It could certainly be provided as a party expert, but not constitute a judicial expert.

40. It is interesting to note that article 220.2 of the Italian Code of Criminal Procedure expressly prohibits (except in the execution phase) psychological examinations of the accused in an attempt to determine the possible existence of a tendency to commit crimes. QUATTROCOLO 2019 highlights how in many States in North America and Australia, predictive software based on psycho-criminal assessments has been used for some time.

41. Integrated into the Institutes of Legal Medicine and Forensic Sciences, by virtue of Organic Law 1/2004, of 28 December, on Comprehensive Protection Measures against Gender Violence.

42. Implemented by Instruction 4/2019 of the Secretary of State for Security, which establishes a new protocol for the police assessment of the level of risk of gender-based violence, the management of the safety of victims and the monitoring of cases through the comprehensive monitoring system for gender-based violence cases.

information provided. This, in turn, is obtained from the responses incorporated into a questionnaire completed by the police, which includes thirty-nine different risk indicators.

It should be noted, however, that it is a predictive system based on algorithms but it is not, strictly speaking, AI⁴³, since this instrument does not use algorithms that “learn” from data processing⁴⁴. In short, it uses statistical models to infer the risk that a victim may run, based on a set of indicators that have been previously determined.

Of course, as will be seen, the system described is very different from the risk assessment carried out in the UVFI and the prognosis that, as we have seen, is made in the execution phase of the criminal process, both of which are characterized by the involvement of multidisciplinary teams of experts. If, even in such cases, it is risky to entrust the judicial decision to an estimated calculation of probabilities (taking into account the unpredictability of human nature), our skepticism about VioGén seems understandable⁴⁵.

We have insisted on the idea that, in relation to any prediction that is made, it is particularly important to pay attention to the data on which it is based. And it is at this point that, we believe, another important objection to VioGén should be raised: some of the information contained in the questionnaire that “feeds” the algorithms on which the prediction is based is, in our opinion, especially delicate. We are referring, in particular, to questions that allude to the existence of jealousy or a desire for control on the part of the partner, clear indicators of a certain personality, if not even of a true psychopathology. Worse still is to ask directly, as is done in the VPR form, about the existence of a mental or psychiatric disorder of the alleged offender. That these notes are taken into consideration only by a computer program, after having been supplied by the alleged victim of the crime (there-

fore, inevitably, subjectively), and that this results in the assessment of a certain level of risk may also lead to the imposition of measures restricting the liberty of the alleged aggressor is hardly acceptable to us. Bearing in mind, moreover, that this diagnosis of dangerousness cannot be contradicted, the right of defense is, in our opinion, as compromised as the presumption of innocence.

The fact that VioGén does not seem to us – at least, as it is configured – to be an adequate channel for the decision on the adoption of measures does not mean, either, that we deny the effectiveness that algorithmic systems, in general, can have in the field of precautionary protection, where they could play a supporting role in the work of the judge, as a particularly useful assessment tool that should not be underestimated. We acknowledge that any initiative in this regard should not only respect the previously mentioned considerations⁴⁶, but also meet an additional requirement: there must be oversight of the types of data utilized. This will support the integrity of algorithmic predictions. In no case do we believe that it is admissible for the application of these programmes to entail the entry into our criminal system of considerations that concern the psychological sphere of the passive subject of the process and that may contribute to forming a criterion about his greater or lesser inclination to crime. Not only should they have no place – for the sake of the presumption of innocence – in the declaratory phase of criminal proceedings, but they should never be assessed exclusively by a computer program. Although VioGén confines itself to making a statistical interpretation of the data provided, without further analysis, it is, in our opinion, a first step in a direction from which we must flee. The algorithmic elaboration of psychological profiling, already present in other areas, must be radically excluded from our justice system.

43. PRESNO LINERA 2023; PÉREZ MARÍN 2023.

44. GONZÁLEZ CABANES-DÍAZ DÍAZ 2023.

45. The Council of Europe’s Group of Experts on Combating Violence against Women and Domestic Violence (GREVIO) evaluated the VioGén system in their [2020 Report](#) on the implementation of the Istanbul Convention in Spain and noted that a significant percentage of women killed by their partners or ex-partners were considered as low-risk cases by the VioGén, which raises the question of whether breaches are taken “too lightly”.

46. Consequently, the last word should be left to a person, there should be room for contradiction between the parties, there should be transparency and publicity of the system used and the judicial motivation should be exhaustive.

5. Discussion

The readers of this paper will learn how algorithms – usually, but not always, linked to AI – are acquiring an increasing importance in the framework of the Administration of Justice, they will know the favorable aspects that this entails and, also, they will be aware of the problems that their use may have in a very specific framework: the criminal precautionary protection. It is in this area where the greatest criticisms of the work will be found. We have used as a paradigmatic example of the above a case that is well known in Spain: the VioGén system. This system involves the application of certain algorithms by the police, in order to determine the risk of repetition of a crime by a detainee arrested for gender violence. As all this translates into the adoption of one or another criminal precautionary measure, it is a clear example of predictive justice.

In short, we have proposed a study that goes from the general (the critical examination of the entry of algorithms into the Administration of Justice) to the particular (their entry into the criminal justice system – at the hands of two of its protagonists: the police and the judges – and, more specifically, in the so-called precautionary measures).

The results obtained in our research are in line with numerous criticisms that – more generally – have been made by the scientific doctrine. Although there are studies that address the impact that the entry of these modern instruments into the Administration of Justice may have on procedural rights and guarantees, the originality of our work lies in having applied these general considerations to a specific scenario: the area of precautionary protection and, more specifically, the VioGén system, about which considerable reticence has been expressed and justified.

It has not been our intention to undertake a comprehensive and exhaustive examination of how the different precautionary measures can be affected, to a lesser or greater extent, by the information that algorithms can provide (which could undoubtedly be the subject of further studies). We have preferred to focus, instead, on the specific examination of what is happening in this regard in the field of gender violence in Spain. As is well known, this is a particularly problematic (and widespread) issue in our country, making the examination of this case especially representative. In our opinion, the way in which the VioGén system

has been developed (especially taking into account the nature of the specific items to be completed), gives rise to significant problems. To this must be added the difficulties already present in any predictive justice system, as we have exposed.

6. Conclusions

Technology is a considerable and increasingly important part of our lives. It is a subject that, without being new, never abandons its relevance. Leaving aside its usefulness as an instrument in almost all spheres of our daily lives (provided that it is properly managed), it would be unfair to deny the wide range of opportunities that, in particular, it offers in the field of law.

From a general perspective, it is undeniable that the application of technology to the process results in accelerated processing, reduced time, and a notable saving of resources. It makes it possible to work with greater efficiency than human efficiency – which is not necessarily linked to effectiveness, as we well know –, which is a remarkable feature in the current state of congestion in the Administration of Justice. Also starting from the perspective of the omnipresent Sustainable Development Goals (especially goal number 16, linked to the promotion of peace, justice and strong institutions), AI could be understood as a particularly valuable resource. In other words, its use for handling such a large amount of data allows us to save time and effort in tasks that, traditionally, have been carried out in a more “artisanal” way. As we have already had occasion to highlight, it is important to insist that these resources should, in any case, be available to all parties to the proceedings, avoiding the inequalities that would arise if only large law firms had access to them.

Regardless of whether algorithms are associated with AI, it is important to recognize that their implementation within the field of the Administration of Justice involves a commitment to safeguarding fundamental rights and guarantees. In this paper we have focused on how the right of defense – and its diverse, multiple, manifestations – are affected by this, could be considered, algorithmic drift, which finds in the so-called “predictive justice” its most striking manifestation.

Assuming all of the above, one of the biggest obstacles to the peaceful acceptance of these new techniques and procedures lies in the way they are

designed and the obscurantism that surrounds them, which makes it extremely difficult to contradict any “algorithmic claim”. The lack of knowledge of the functioning of such algorithms on the part of the citizen, which prevents questioning not only their mere creation but also the selection that – unavoidable – underlies the information from which they are nourished, brings with it the risk of their incontestability. We must not forget that in our model of criminal procedure there is a system of free evaluation of evidence that is diametrically distant from the possible consideration of the data provided by these algorithms as weighted evidence. Nor should the presumption of the veracity of algorithmic readings prevail, which would result in a *de facto* shift of the burden of proof to the accused and, consequently, in an unacceptable compromise of the rights of defense. Human control over the operation of the algorithm will be as necessary as the possibility of deviate from the solution it proposes. The judicial statement of reasons for their action will also be essential.

The lack of knowledge of multiple facets relating to the creation and operation of such algorithms limits – it seems beyond doubt – the effective exercise of the rights of defense. Not only will it be impossible to confront a decision (precautionary or otherwise) that is based on an algorithmic prediction of uncertain origin and operability – which is a clear violation of the principle of contradiction

– but the very filing of appeals against it would be meaningless. The right to effective judicial protection would, in short, be seriously affected. It would not be unreasonable to venture, given the circumstances, that the famous *Loomis* case will be only the first of many.

An important part of our attention has been drawn to the examination of VioGén, as a paradigmatic example of a system based on predictive algorithms. In this sense, it is not only the data or the information used by the system – which, as we said, has some characteristics of psychopathological tests – that concerns us; it is also the way in which the system is set up, the training of those who have to assess the result it produces and the absence of expert supervision before the result obtained is passed on to the judge. We must reiterate this point: it is essential to avoid basing the adoption of a measure (whether precautionary or definitive) on forecasts that consider a hypothetical personal predisposition to commit a crime, particularly when such forecasts are the automatic outcome of an algorithmic application that utilizes data potentially indicative of certain personality traits, including psychopathological ones.

In light of the above, it is crucial to continue advancing in the development of fundamental requirements that underpin a rational and proportionate use of algorithms, particularly within the framework of criminal justice.

References

- S. BARONA VILAR (2021), *Algoritmización del derecho y de la justicia. De la inteligencia artificial a la Smart Justice*, Tirant lo Blanch, 2021
- F. BASILE (2019), *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in “Diritto Penale e Uomo”, 2019
- R. BRIGHI (2016), *Su statuto epistemologico e consolidamento tecnico-giuridico dell’informatica forense*, in “Anales de la Facultad de Derecho”, Universidad de La Laguna, 2016, n. 33
- CEPEJ (EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE) (2019), *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, 2019
- CTEAJE (COMITÉ TÉCNICO ESTATAL DE LA ADMINISTRACIÓN JUDICIAL ELECTRÓNICA) (2022), *Manifiesto por un espacio público de datos en el ámbito de justicia*, 2022
- G. CONTISSA, G. LASAGNI, G. SARTOR (2019), *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in “Diritto di Internet”, 2019, n. 4
- L. COTINO HUESO (2017), *Big Data e Inteligencia Artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales*, in “Dilemata”, 2017, n. 24

- Y. CUI (2019), *Artificial Intelligence and Judicial Modernization*, Springer, 2019
- B.H.M. CUSTERS (2022), *AI in Criminal Law: An Overview of AI Applications in Substantive and Procedural Criminal Law*, in B.H.M. Custers, E. Fosch Villaronga (eds.), "Law and Artificial Intelligence", Springer, 2022
- A. DEL MORAL GARCÍA (2023), *Inteligencia artificial y justicia penal*, in "I Simposio Justicia y derecho en Datos", Ministerio de Justicia 2023
- F. DONATI (2020), *Intelligenza Artificiale e Giustizia*, in "Rivista AIC", 2020, n. 1
- F.J. FERNÁNDEZ GALARRETA (2021), *Derecho de defensa e inteligencia artificial. Reflexión crítica acerca de la repercusión de la inteligencia artificial en la profesión de abogado*, in A.I. Pérez Machío, J.L. De la Cuesta Arzamendi (dirs.), "Contra la política criminal de tolerancia cero", Aranzadi, 2021
- M.D. GARCÍA SÁNCHEZ (2023), *El necesario balance entre la heurística algorítmica y judicial como garantía de los derechos procesales del justiciable; hacia una inteligencia artificial explicable*, in P. Martín Ríos, C. Villegas Delgado (dirs.), "La tecnología y la inteligencia artificial al servicio del proceso", Colex, 2023
- M.D. GARCÍA SÁNCHEZ (2022), *Big brother ¿Ciencia ficción o realidad?*, in "Ius et Scientia", 2022, n. 8
- L. GIACOMELLI (2019), *Big brother is «gendering» you. Il diritto antidiscriminatorio alla prova dell'intelligenza artificiale: quale tutela per il corpo digitale?*, in "BioLaw Journal – Rivista di BioDiritto", 2019, n. 2
- J.L. GONZÁLEZ ÁLVAREZ, J. SANTOS HERMOSO, M. CAMACHO COLLADOS (2020), *Policía predictiva en España: aplicación y retos futuros*, in "Behavior & Law Journal", 2020, n. 6
- F. GONZÁLEZ CABANES, N. DÍAZ DÍAZ (2023), *¿Qué es la Inteligencia Artificial?*, in E. Gamero Casado, F. Pérez Guerrero (dir./coord.), "Inteligencia artificial y sector público. Retos, límites y medios", Tirant lo Blanch, 2023
- A.Z. HUQ (2019), *Racial Equity in Algorithmic Criminal Justice*, in "Duke Law Journal", vol. 68, 2019, n. 6
- F. MARTÍN DIZ (2021), *Herramientas de inteligencia artificial y adecuación en el ámbito del proceso judicial*, in L. Bujosa Vadell (dir.), "Derecho procesal: retos y transformaciones", Atelier, 2021
- I. MARTÍNEZ MONTENEGRO (2023), *Sobre los métodos de la investigación jurídica*, in "Revista chilena de Derecho y Ciencia política", vol. 14, 2023, n. 1
- P. MOSCARINI (2015), *Lo statuto della "prova scientifica" nel processo penale*, in "Diritto Penale e Processo", 2015, n. 6
- D. MURAKAMI WOOD (ed.) (2006), *A Report on the Surveillance Society*, September 2006
- J. NIEVA FENOLL (2018), *Inteligencia Artificial y proceso judicial*, Marcial Pons, 2018
- P.P. PAULESU (2023), *Inteligencia Artificial y proceso penal italiano: una panorámica*, in P. Martín Ríos, C. Villegas Delgado (dirs.), "La tecnología y la inteligencia artificial al servicio del proceso", Colex, 2023
- M.J. PÉREZ ESTRADA (2019), *El uso de algoritmos en el proceso penal y el derecho a un proceso con todas las garantías*, in S. Barona Vilar (dir.), "Claves de la Justicia Penal. Feminización, Inteligencia Artificial, Supranacionalidad y Seguridad", Tirant lo Blanch, 2019
- M.Á. PÉREZ MARÍN (2023), *Violencia de género y algoritmización: la justa medida del sistema VioGén*, in D. Vallespín Pérez (dir.), "Algoritmización de la justicia penal", Juruá, 2023
- M.A. PRESNO LINERA (2023), *Policía predictiva y prevención de la violencia de género: el sistema VioGén*, in "Revista de Internet, Derecho y Política", 2023, n. 39
- S. QUATTROCOLO (2020), *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Springer, 2020

- S. QUATTROCOLO (2019), *Equo processo penale e sfide della società algoritmica*, in “BioLaw Journal. Rivista di BioDiritto”, 2019, n. 1
- J.L. RODRÍGUEZ LAINZ (2023), *Prólogo*, in P. Martín Ríos, C. Villegas Delgado (dirs.), “La tecnología y la inteligencia artificial al servicio del proceso”, Colex, 2023
- C. SAN MIGUEL CASO (2021), *La aplicación de la Inteligencia Artificial en el proceso: ¿un nuevo reto para las garantías procesales?*, in “Ius et Scientia”, 2021, n. 7
- P. SIMÓN CASTELLANO (2021), *Inteligencia artificial y Administración de Justicia: ¿Quo vadis, justitia?*, in “Revista de Internet, Derecho y Política”, 2021, n. 33
- D. VALLESPÍN PÉREZ (2023), *Inteligencia Artificial y Proceso: eficiencia vs. garantías*, Juruá, 2023
- D. VALLESPÍN PÉREZ (2022), *Intelligenza Artificiale e valutazione delle prove nel processo civile spagnolo e italiano*, in “Revista General de Derecho Procesal”, 2022, n. 57
- C. VILLEGAS DELGADO (2023), *Gobernanza algorítmica, ética de la inteligencia artificial y estado (algorítmico) de derecho. Retos para el jurista en la era digital*, in D. Vallespín Pérez (dir.), “Inteligencia Artificial y Proceso: eficiencia vs garantías”, Juruá, 2023
- P. ŽIVKOVIĆ, R. DUCATO (2023), *Algorithmic discrimination: a blueprint for a legal análisis*, EU and Comparative Law Issues and Challenges Series (ECLIC), 2023, n. 7



GIANLUCA FASANO

L'interpretazione estensiva della nozione di "decisione automatizzata" ad opera della Corte di giustizia: una prospettiva più ampia ma ancora fragili tutele per le libertà fondamentali

Utilizziamo sempre di più artefatti non per facilitare il compimento di un'azione, un'attività o un'operazione che abbiamo già pianificato, bensì per assumere decisioni. La delega compu-decisionale varia significativamente a seconda della complessità delle decisioni da assumere, del livello di automazione e del corrispondente grado dell'intervento umano. E proprio sul rapporto tra grado di automazione e intervento umano che si incentrano le tutele previste dal Regolamento europeo sul trattamento dei dati personali. Tuttavia, subordinare le tutele normative ad un'indagine circa la complessità delle diverse dinamiche che caratterizzano i processi decisionali automatizzati, alla ricerca di evidenze sulla prevalenza dell'uno o dell'altro fattore in contesti formati da reti complesse di input, algoritmi, dati e interventi umani, rischia di dissolvere le tutele stesse. La recente sentenza della Corte di giustizia (C-634/21, *Schufa*) pur offrendo un'interpretazione estensiva della nozione di decisione automatizzata, consente di mettere in luce, ancora una volta, le fragilità delle tutele costruite per le libertà fondamentali.

Sistemi decisionali automatizzati – Scoring – Intelligenza artificiale – Dati personali

The Court of Justice's broad interpretation of the notion of "automated decision-making": a broader perspective but still fragile protections for fundamental rights

More and more common artifacts are used not to facilitate the completion of an action, activity or operation that we have already planned, but rather to make decisions. The compu-decisional delegation varies significantly depending on the complexity of the decisions to be made, the level of automation and the corresponding degree of human intervention. The protections provided by the European Regulation on the processing of personal data focus precisely on the relationship between the degree of automation and human intervention. However, to subordinate legal protections to an investigation into the complexity of the different dynamics that characterize automated decision-making processes, in search of evidence on the prevalence of one or the other factor in contexts formed by complex networks of inputs, algorithms, data and human interventions, it may lower the legal protections. The recent judgment of the Court of Justice (C-634/21, *Schufa*), while offering an extensive interpretation of the notion of automated decision, allows us to highlight, once again, the fragility of the protections built for fundamental rights.

Automated decision-making – Scoring – Artificial intelligence – Personal data

SOMMARIO: 1. Introduzione. – 2. La nozione di decisione automatizzata ai sensi dell'art. 22 Gdpr. – 3. L'interpretazione espansiva della Corte di giustizia dell'Unione europea (C-634/21, *Schufa*). – 4. I riflessi della sentenza sulla tutela delle libertà fondamentali. – 5. Conclusioni.

1. Introduzione

L'avvento dei "processi decisionali automatizzati" (*Automated Decision-Making*)¹, grazie a macchine dotate di ampie capacità di calcolo in riferimento a enormi quantità di dati, ha rivoluzionato numerosi aspetti della nostra società, influenzando in maniera significativa le modalità con cui vengono prese decisioni cruciali nella (e per) la vita di tutti i giorni. Essi vengono utilizzati in una vasta gamma di settori dove è necessario analizzare una grande quantità di informazioni al fine di valutare, prevedere e prendere decisioni. Si pensi al settore bancario e finanziario², ove sono diffusi per valutare il rischio di credito di un individuo o di un'azienda, indirizzando la decisione sul se concedere un prestito, a quale tasso di interesse e a quali condizioni. Di impieghi ne troviamo anche nel settore assicurativo³, ove le compagnie possono utilizzarli per determinare i premi assicurativi, nel settore immobiliare, dove i proprietari possono valutare la solvibilità dei potenziali inquilini, nel mercato del lavoro, in cui i datori di lavoro possono utilizzarli nel processo di screening dei candidati, sia per il

reclutamento che per la progressione professionale, e perfino nel settore pubblico, ove possono esser impiegati per decidere l'erogazione di servizi⁴. Per citarne solo alcuni.

In tali contesti, i processi decisionali automatizzati utilizzano algoritmi di *scoring*, il cui obiettivo è quello di valutare il rischio comportamentale di un individuo, sulla base di criteri predeterminati, di classi di individui precostituite, di procedure di profilazione, al fine di attribuirgli un livello di affidabilità nell'ambito di un determinato scenario futuro. I processi decisionali non sono soltanto questo, poiché non sempre si caratterizzano per il ricorso a strumenti computazionali sofisticati. Anche con semplici algoritmi è possibile dar luogo a una decisione automatizzata, quello che muta è il livello di automazione che si intende raggiungere e il grado di intervento dell'essere umano. Un impiego di tal tipo, per esempio, ha riguardato i procedimenti di mobilità dei docenti scolastici, attuati ai sensi della legge n. 107/2015 (c.d. "Buona scuola"), in cui il Ministero dell'Istruzione ha utilizzato un semplice algoritmo per individuare la sede di destinazione dei docenti scolastici⁵.

1. Per seguire il lessico contenuto nel Regolamento (UE) 2016/679, Regolamento generale sulla protezione dei dati personali.
2. BIFERALI 2018, p. 487 ss.
3. PORRINI 2018, p. 319 ss.
4. Sull'uso di sistemi decisionali automatizzati nel settore dei pubblici servizi è noto il caso SyRI, sistema automatizzato progettato nei Paesi Bassi per combattere le frodi in materia di previdenza sociale, giudicato dal tribunale distrettuale dell'Aia (*Rechtbank Den Haag* 5 febbraio 2020, C-09-550982-HA 18-388) in contrasto con l'articolo 8 della Convenzione europea dei diritti dell'uomo (CEDU). Vedi APPELMAN-FATHAIGH-VAN HOBOKEN 2022.
5. La serie di pronunce della giustizia amministrativa riferite ai procedimenti di mobilità della c.d. "Buona scuola" (da ultimo Cons. Stato, Sez. VI, 13 dicembre 2019, n. 8472) ha riaperto l'attenzione sulle teorie profilate

Dunque, un'automazione finalizzata a velocizzare l'istruttoria amministrativa di una moltitudine di istanze avanzate da dipendenti e disciplinate da una normativa molto dettagliata.

Nonostante la varietà di impieghi e di complessità dei modelli adottati, possiamo identificare un ruolo e una connotazione peculiare di tali sistemi, ai quali non chiediamo semplicemente di compiere un'azione, un'attività o un'operazione che abbiamo già pianificato e deciso, bensì chiediamo di assumere decisioni. Si tratta di una nuova categoria di artefatti, non tradizionali potremmo dire, ovvero utilizzati non come mezzi per consentire all'uomo di ottenere un risultato atteso, previsto e già deciso, bensì per prendere decisioni senza la necessità di un intervento umano diretto. Tale aspetto assume particolare rilevanza nell'attuale contesto tecnologico, caratterizzato da un'accelerata evoluzione delle nuove tecnologie, comprese quelle legate all'intelligenza artificiale (AI)⁶.

La delega decisionale può essere modellata per rispondere a una vasta gamma di contesti e obiettivi – impliciti ed espliciti – e in base alle esigenze specifiche del caso concreto. A seconda della complessità delle decisioni da prendere, varia significativamente il livello di automazione e il corrispondente grado dell'intervento umano⁷. Proprio sul rapporto tra grado di automazione e intervento umano si incentra la disciplina dettata dall'art. 22 del Regolamento UE n. 2016/679, “relativo alla protezione delle persone fisiche con riguardo al

trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE” [d'ora in poi anche Gdpr] in breve tempo divenuto un punto di riferimento fondamentale per garantire la tutela dei diritti e delle libertà fondamentali degli individui nel campo dei processi decisionali automatizzati. All'indomani dell'approvazione del Regolamento, invero, una delle questioni più dibattute è stata quella dell'interpretazione del citato articolo⁸ che, oggi, riceve nuova linfa per via della prospettiva “espansiva” offerta dalla Corte di giustizia dell'Unione europea (causa C-634/21, *Schufa*). La decisione merita attenzione per diversi motivi che cercheremo di esplorare nel seguito di questo lavoro, evidenziando le sue implicazioni per la protezione dei dati personali, l'autonomia decisionale e la responsabilità delle organizzazioni.

2. La nozione di decisione automatizzata ai sensi dell'art. 22 Gdpr

Il principale riferimento normativo in materia è rappresentato dall'art. 22 del Gdpr, il quale introduce una tutela per le persone fisiche sulla base del concetto di non esclusività della decisione automatizzata: «l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona»⁹.

dalla dottrina in merito all'utilizzo di modelli decisionali automatizzati nella funzione amministrativa. Nella fattispecie, i ricorrenti, docenti della scuola secondaria di secondo grado rientranti nel piano straordinario di assunzione a tempo indeterminato, lamentavano che a causa di un algoritmo di cui non si conoscerebbero le concrete modalità di funzionamento le assegnazioni delle sedi non avevano rispettato criteri ispirati al principio meritocratico, fondamentale nel reclutamento del personale per l'accesso al pubblico impiego. In particolare, essi contestavano che docenti collocati in graduatoria in posizione peggiore avrebbero beneficiato di maggior tutela, per esser stati assunti assecondando le preferenze circa le classi di concorso e le province di residenza.

6. AMATO MANGIAMELI 2023, pp. 275-280.

7. Cfr. OECD 2024, in cui, relativamente ai sistemi di AI, è presente questa definizione di autonomia «AI system autonomy (contained in both the original and the revised definition of an AI system) means the degree to which a system can learn or act without human involvement following the delegation of autonomy and process automation by humans».

8. WACHTER-MITTELSTADT-FLORIDI 2017.

9. Art. 22, par. 1, del Gdpr. Secondo le Linee guida sulle decisioni automatizzate individuali adottate il 7 ottobre 2017 dal Gruppo di lavoro sulla protezione degli individui con riguardo al trattamento dei dati personali istituito dall'art. 29 della direttiva 95/46/EC (c.d. “A29WP”), anche un annuncio pubblicitario “personalizzato” può essere una decisione agli effetti dell'art. 22.

La norma sancisce un espresso divieto a carico del titolare del trattamento e, nell'ottica della tutela *by default* sancita dal Gdpr, non richiede comportamenti di sorta da parte dell'interessato, il quale non è onerato di alcunché affinché la tutela abbia luogo¹⁰.

Sul piano applicativo, al fine di poter invocare la tutela normativa occorre individuare l'esatto confine della fattispecie di divieto, compito che non risulta affatto agevole alla luce dei due parametri normativi che fondano il divieto stesso: il legame della decisione con il trattamento automatizzato, che deve esser qualificato da una connessione forte come risulta dall'espressione «unicamente»; e l'efficacia della decisione che può manifestarsi nella produzione di «effetti giuridici» ovvero nell'incidere «significativamente» sulla persona. Dunque, già dalla lettera della norma possiamo trarre l'idea di un ambito applicativo segnato da limiti sì pregnanti ma le cui sfumature danno adito a non poche questioni interpretative e che, in definitiva, consentono di indugiare sulla sua effettiva portata applicativa.

Guardiamo al primo parametro, quello dell'intervento umano: il divieto scatta qualora la decisione sia basata «unicamente sul trattamento automatizzato, compresa la profilazione». La norma sembra ricercare una connessione univoca tra l'elaborazione automatizzata – di aspetti personali – e l'atto decisionale, tale da poter giudicare quest'ultimo come frutto diretto ed esclusivo della prima, quasi in un rapporto di causa ed effetto. Il divieto non mira ad assicurare che vi sia sempre e comunque un elemento umano nel processo decisionale poiché il legislatore è consapevole che rinunciare del tutto all'efficienza derivante dall'automazione significa rinunciare all'innovazione. Per questo, il divieto non opera laddove la procedura automatizzata rivesta un ruolo secondario nella produzione dell'atto decisionale

ovvero qualora, pur in presenza di una decisione unicamente automatizzata, ricorrano le deroghe della conclusione o esecuzione di un contratto tra l'interessato e un titolare del trattamento (par. 2, lett. a); del diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento (par. 2, lett. b); del consenso esplicito dell'interessato (par. 2, lett. c). Ma, in tutti questi casi, comunque operano delle restrizioni finalizzate ad innalzare il livello di tutela del diritto alla protezione dei dati personali (parr. 3 e 4).

La *ratio* della disposizione, quindi, non andrebbe ricercata nella preoccupazione che l'affidamento esclusivo su algoritmi o modelli computazionali potrebbe portare a decisioni ingiuste o discriminatorie, quanto nell'approccio che ispira la disciplina europea sulla protezione dei dati personali, volta a legittimare la circolazione dei dati personali per promuovere lo sviluppo del mercato unico digitale assicurando, al contempo, che le persone abbiano un controllo sui propri dati personali¹¹. Ma proprio la ricerca di questo equilibrio poggia su elementi sfuggenti e complessi da individuare, tanto per il titolare del trattamento, a cui la logica dell'*accountability* che informa l'intera disciplina del Gdpr rimette la discrezionalità di tale *assessment*, quanto per l'interessato in sede di tutela *ex post*. Indagare la misura in cui il calcolo computazionale sia prevalente sull'elemento umano è essenziale per poter invocare le tutele normative avverso le decisioni basate esclusivamente sul trattamento automatizzato e che potrebbero avere conseguenze significative per le proprie vite. Eppure un'indagine circa la prevalenza dell'uno o dell'altro fattore in contesti molto complessi, fatti di reti di input, algoritmi, dati e influenze umane, rischia di dissolvere le tutele stesse.

Anche il parametro dell'incidenza significativa della decisione sulla persona non è di facile valutazione. Anzitutto, la stessa formula della norma

10. L'art. 15 della direttiva 95/46/CE sulla protezione dei dati prevedeva un diritto simile. Per una panoramica sulle differenti normative nazionali di recepimento si veda KORFF 2002, p. 106 ss.

11. RODOTÀ 1995, p. 34. Per l'Autore «si può dire che oggi la sequenza quantitativamente più rilevante è quella “persona-informazione-circolazione-controllo”, e non più soltanto “persona-informazione-segretezza”, intorno alla quale è stata costruita la nozione classica di privacy. Il titolare del diritto alla privacy può esigere forme di “circolazione controllata”, e non solo interrompere il flusso delle informazioni che lo riguardano». Il Gruppo di lavoro Articolo 29 lega la libertà del consenso alla possibilità di avere il controllo dei dati personali, sostenendo che «se ottenuto nel pieno rispetto del regolamento, il consenso è uno strumento che fornisce all'interessato il controllo sul trattamento dei dati personali che lo riguardano», GRUPPO DI LAVORO ARTICOLO 29 2020, 3.

non offre criteri oggettivi attraverso cui valutare quando una decisione sia destinata ad incidere “significativamente” sulla persona dell’interessato¹². Ancora una volta, la mancanza di criteri oggettivi sarà supplita da criteri soggettivi, cioè, affidando siffatta valutazione al titolare del trattamento, nella logica dell’*accountability*. Tuttavia, la sua valutazione sarà comprensibilmente rivolta a uno standard in cui non tutte le persone (interessati) potrebbero identificarsi, per via dei loro differenti gradi di vulnerabilità e per via del fatto che il concetto di dignità della persona non è comprimibile in standard omogenei. Per tali ragioni, l’interessato si troverebbe costretto a dover eccepire le proprie ragioni opponendosi alla decisione automatizzata, soltanto *ex post*, a decisione assunta e sacrificio ormai prodotto.

Per di più, ci sono casi in cui la incisività della decisione automatizzata è celata agli occhi dell’interessato per cui viene a mancare anche quell’ultimo baluardo di garanzia rappresentato dall’autodifesa. Si pensi alla pubblicità mirata che, apparentemente non incisiva dal momento che può essere ignorata, influenza il punto di vista e la libertà di scelta degli utenti. Attraverso messaggi inviati ai singoli individui, e personalizzati grazie a sofisticati modelli predittivi computazionali di micromarketing¹³, di cui la maggior parte degli utenti ignora l’esistenza e il funzionamento, si creano delle vere e proprie *filter bubbles*¹⁴, ovvero delle bolle in cui l’utente viene rinchiuso ricevendo soltanto informazioni conformi alle proprie opinioni e pregiudizi¹⁵.

La consapevolezza che si tratta di una previsione di difficile interpretazione ha spinto l’interprete, da più fronti, a individuare elementi o standard che ne potessero agevolare la qualificazione.

Il Gruppo di lavoro Articolo 29, per esempio, ha identificato almeno due elementi da considerarsi rappresentativi di un intervento umano: che il coinvolgimento umano sia opera di «una persona che dispone dell’autorità e della competenza per modificare la decisione» e che «tale persona dovrebbe prendere in considerazione tutti i dati pertinenti»¹⁶. Di certo la capacità della persona di poter assumere e sindacare il risultato del modello computazionale è un indice sintomatico della astratta riconducibilità della decisione all’operato umano. Tuttavia, resta il dubbio sull’ulteriore elemento, quello inerente a una persona che, per quanto autorevole e competente, possa «prendere in considerazione tutti i dati pertinenti», cioè tutti i dati che soltanto sofisticati sistemi di calcolo sono in grado di analizzare ed elaborare.

Nello stesso senso si è mosso anche il Parlamento europeo che nella Risoluzione sugli aspetti etici dell’intelligenza artificiale (20 ottobre 2020) evidenzia che nei casi in cui siano in gioco le libertà fondamentali gli Stati membri dovrebbero ricorrere a tali tecnologie soltanto «quando sono possibili o sistematici un intervento e una verifica sostanziali da parte dell’uomo». Nell’ambito medico e dell’assistenza sanitaria il Parlamento europeo è stato più risoluto, ritagliando alle decisioni automatizzate un ruolo di supporto strumentale alla

12. Un’indicazione viene fornita nei Considerando (n. 71) laddove si cita a titolo esemplificativo «il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani». Anche il GRUPPO DI LAVORO ARTICOLO 29 2020, 24, è intervenuto sull’argomento, enucleando quali situazioni significative quelle che influenzano le condizioni finanziarie di una persona (ammissibilità al credito), ovvero l’accesso ai servizi sanitari, che negano un’opportunità di impiego o pongono tale persona in una posizione di notevole svantaggio; decisioni che influenzano l’accesso di una persona all’istruzione, ad esempio le ammissioni universitarie.

13. Il *microtargeting* è una tecnica che analizza i dati personali per prevedere gli interessi di un pubblico specifico: una pratica che costituisce il modello di business fondamentale di diverse grandi piattaforme di social media e che è diventata nota al grande pubblico con lo scandalo Cambridge Analytica del 2016.

14. PARISIER 2011, e più di recente SHAFFER 2019; LONGO 2019, p. 29 ss.

15. Sulla questione si è pronunciato anche il garante della protezione dei dati dell’Ue (GEPD) sulle proposte della Commissione europea per il *Digital Services Act* (DSA) e il *Digital Markets Act* (DMA), per il quale «Data la moltitudine di rischi associati alla pubblicità mirata online, il GEPD esorta i legislatori a prendere in considerazione norme aggiuntive che vadano oltre la trasparenza».

16. GRUPPO DI LAVORO ARTICOLO 29 2020, 23.

decisione presa dall'agente umano. Si tratta di un campo in cui i modelli decisionali automatizzati svolgono un ruolo sempre più cruciale, si pensi agli algoritmi di supporto alla diagnosi, la chirurgia robotica, le protesi intelligenti e i robot sociali per l'assistenza agli anziani, la cui diffusione potrebbe inficiare la parità di trattamento dei pazienti in termini di accesso alle cure e alterare il rapporto tra paziente e medico. Nella Risoluzione del 20 gennaio 2021 il Parlamento ha voluto stigmatizzare la responsabilità del professionista evidenziando come egli deve aver sempre presente la possibilità di discostarsi dalla soluzione proposta dall'AI¹⁷. La questione viene così affrontata dal punto di vista della responsabilità, quasi a monito di un utilizzo spesso ossequioso e conformativo alle risultanze del sistema automatizzato.

Ed è questo un aspetto fondamentale da considerare. Anche quando la decisione non è basata unicamente sul trattamento automatizzato di aspetti personali, cioè quando il ruolo del soggetto umano appare rilevante ai fini dell'assunzione della decisione, quando il divieto ex art. 22 non trova applicazione, ci possiamo aspettare che la «travolgente forza pratica dell'algoritmo»¹⁸ prevalga, di fatto, sulla valutazione dell'uomo. Sebbene venga prestata notevole attenzione affinché le decisioni non siano affidate soltanto all'algoritmo ma contemplino anche un coinvolgimento umano non è da sottovalutare quella capacità dell'algoritmo di indurre il decidente ad affidarsi all'esito

computazionale e ad assumere la decisione restando passivamente l'esito computazionale.

Gli sviluppi esponenziali delle capacità di calcolo delle nuove tecnologie, in particolare delle macchine intelligenti, presenteranno sempre più spesso artefatti con capacità di analisi e inferenziali indispensabili per l'uomo. Le ragioni per affidare alcune attività a sistemi automatizzati saranno sempre più sostenute e predominanti: vantaggi di elaborazione dati su larga scala, velocità, volume e aspettative di tassi di errore inferiori rispetto agli esseri umani. Di fondo, viene riconosciuta alle macchine una maggiore efficienza rispetto alle capacità analitiche umane: gli algoritmi sono infatti in grado di analizzare quantità elevatissime di dati, anche fra loro eterogenei sotto il profilo qualitativo, individuandone preziose correlazioni, rapporti, inferenze che nessuna valutazione umana sarebbe in grado di rilevare¹⁹. Il rapporto tra atto decisionale ed elaborazione automatizzata di aspetti personali sarà sempre più arduo da esplorare e, nonostante gli sforzi interpretativi, l'effettività delle tutele previste dall'art. 22, il cui discrimine è nella prevalenza del fattore automazione, resterà confinata in un perimetro sfuggente²⁰.

3. L'interpretazione espansiva della Corte di giustizia dell'Unione europea (C-634/21, *Schufa*)

La recente pronuncia della Corte di giustizia, declinata con particolare riferimento all'impiego del

17. Risoluzione del Parlamento europeo del 20 gennaio 2021 sull'intelligenza artificiale, par 65.

18. SIMONCINI 2019, p. 81, che puntualizza come tale forza non dipenda da ragioni di valore scientifico, di accuratezza predittiva o di affidabilità tecnica dell'automatismo, ma – appunto – da mera convenienza pratica.

19. Contraria è la posizione del TAR Lazio, sent. 10 settembre 2018, n. 9227, il quale ha relegato l'uso di decisione completamente automatizzare nell'ambito dell'istruttoria amministrativa ad un «ruolo strumentale e meramente ausiliario dell'attività dell'uomo» stabilendo che «le procedure informatiche, finanche ove pervengano al loro maggior grado di precisione e addirittura alla perfezione, non possano mai soppiantare, sostituendola davvero appieno, l'attività cognitiva, acquisitiva e di giudizio che solo un'istruttoria affidata ad un funzionario persona fisica è in grado di svolgere». Sul rapporto tra PA e AI, GALETTA-CORVALÁN 2019. Sia consentito infine richiamare FASANO 2020.

20. La Commissione europea, nella Comunicazione *Building Trust in Human-Centric Artificial Intelligence*, doc. COM(2019)168, 8 aprile 2019, 4, al fine di circoscrivere uno spazio di intervento dell'uomo ha individuato almeno tre diverse intensità: «*Human-in-the-loop*» l'intervento umano in ogni ciclo decisionale del sistema; «*Human-on-the-loop*» l'intervento umano a monte del design del sistema e durante il suo funzionamento; «*Human-in-command*» l'intervento capace di decidere come e quando usare l'AI in una situazione particolare. V. anche AMOROSO-TAMBURRINI 2019; BYGRAVE 2001, p. 20; MALGIERI-COMANDÉ 2017, p. 251.

credit scoring (C-634/21, *Schufa*)²¹, merita attenzione per diversi motivi: anzitutto, perché si inserisce nel dibattito stimolato in dottrina circa l'individuazione di esatti confini applicativi del divieto; poi, dacché apporta una prospettiva espansiva della nozione giuridica di "decisione automatizzata"; e, infine, per i riflessi che essa comporterà, al di là del caso concreto di *credit scoring*, per la comprensione del grado di effettività delle tutele per i diritti e le libertà fondamentali. La decisione è destinata a far discutere a lungo, inserendosi in un ambito, quello dell'interpretazione dell'art. 22 del Gdpr, che sarà sempre più difficile da indagare per via della complessità dei processi che concorrono alla formazione delle decisioni automatizzate.

Per maggiore chiarezza espositiva pare opportuno riepilogare per cenni la vicenda giudiziaria decisa dal citato provvedimento. La *Schufa Holding* è una società privata di diritto tedesco che fornisce ai suoi partner contrattuali informazioni sul merito creditizio di terzi, in particolare di consumatori. A tal fine, essa stabilisce un pronostico sulla probabilità di un comportamento futuro di una persona (score), come il rimborso di un prestito. La solvibilità della persona viene calcolata, grazie a procedure matematiche e statistiche, utilizzando dati e caratteristiche personali che provengono da svariate fonti, quali conti bancari, cronologia degli acquisti online e informazioni pubbliche, come le decisioni pubblicate nelle procedure di insolvenza. Sulla base di tale profilazione individuale, che si fonda sul vissuto pregresso dell'individuo, viene rilasciato un certificato che attesta un punteggio di merito. Chi ha un punteggio alto è considerato un buon debitore ed è considerato affidabile in caso di concessione di ulteriori obbligazioni come prestiti, mutui bancari, locazione di case e anche per accedere a servizi telefonici e Internet.

Come venga calcolato il punteggio effettivo, tuttavia, non è argomento noto e la decisione in oggetto deriva proprio dal rifiuto della *Schufa Holding* di fornire informazioni sui loro metodi di attribuzione del punteggio. Ne è scaturito,

dapprima, un reclamo dinanzi all'autorità tedesca per la protezione dei dati e, poi, un ricorso dinanzi al Verwaltungsgericht Wiesbaden (Tribunale amministrativo di Wiesbaden, Germania), il quale ha deciso di sospendere il procedimento e di sottoporre alla Corte di giustizia la seguente questione pregiudiziale: la decisione di negare il credito da parte di una banca sulla base del punteggio di credito elaborato della *Schufa* rientra nel campo di applicazione dell'articolo 22 Gdpr?

La particolarità del caso discende dalla circostanza, non di poco rilievo, che il processo decisionale ha coinvolto più attori, da un lato, la *Schufa* che ha calcolato il punteggio di merito, dall'altro, la banca che ha deciso di negare il credito sulla base di tale profilazione. In considerazione di ciò, la questione pregiudiziale assume contorni più articolati, involgendo il dibattito sul se costituisce una decisione automatizzata, ai sensi dell'art. 22 Gdpr, il tasso di probabilità basato su dati personali relativi a una persona e riguardante la capacità di quest'ultima di onorare impegni di pagamento in futuro, qualora tale tasso di probabilità venga comunicato ad un soggetto terzo che, a sua volta, assume la decisione di stipulare, eseguire o cessare un rapporto contrattuale con tale persona.

Secondo la tesi illustrata nell'interesse della *Schufa*, essa si limitava a far pervenire informazioni alle sue controparti contrattuali senza intervenire direttamente nella decisione. Erano queste ultime ad adottare le decisioni negoziali propriamente dette. Secondo questa tesi, la *Schufa* agirebbe semplicemente come intermediario di informazioni, senza interferire nella decisione finale che resta appannaggio esclusivo delle controparti contrattuali, come le banche, le istituzioni finanziarie o altri soggetti.

Sul piano formale la tesi appare solidamente costruita, posto che certamente la *Schufa* non esercita un potere proprio sulle transazioni finanziarie/contrattuali ma si limita ad aiutare terzi a valutare il rischio creditizio associato alle loro controparti potenziali²². Tuttavia, sebbene ciò risponda a una

21. Corte di giustizia dell'Unione europea, sentenza 7 dicembre 2023, *Schufa Holding AG*, C-634/21, ECLI:EU:C:2023:957. Nell'occasione la Corte ha pronunciato una seconda sentenza che pertiene alle Cause riunite C-26/22 e C-64/22 ove viene indagato il tema della liceità del trattamento dei dati una volta raccolti nella banca dati *Schufa*.

22. In linea con la propria posizione, la *Schufa*, ricevute le richieste di accesso da parte degli interessati, si limitava ad esporre a grandi linee le modalità di calcolo dei punteggi ma, invocando il segreto commerciale, si rifiutava

visione coerente dei ruoli contrattuali coinvolti, non appare convincente sul piano dell'allocazione effettiva del potere decisionale automatizzato.

Per comprendere appieno la decisione della Corte occorre tenere a mente questa prospettiva, non perché sia fondata, ma perché è sulla base di essa che viene articolato il percorso argomentativo, plasmato dalla particolarità del caso concreto che vede più attori coinvolti nella decisione²³. Per la soluzione della questione pregiudiziale, quindi, si è reso necessario stabilire dove è allocato il potere decisionale nell'ambito del fenomeno dell'algoritmo di *scoring*.

La ricostruzione della Corte procede per gradi. Dapprima, viene chiarita la nozione giuridica di "decisione" che, seppur non contenuta nel Regolamento, trae dalla formulazione della norma una prima indicazione: è decisione qualsiasi attività atta a produrre «effetti giuridici... o che incida in modo analogo significativamente sulla ... persona». Tale lettura trova il conforto nel considerando 71, ai sensi del quale una decisione può consistere anche in «una misura, che valuti aspetti personali ... e che produca effetti giuridici ... o incida in modo analogo significativamente sulla sua persona». Per di più, il medesimo considerando procede con esempi specifici, riferendosi proprio al «rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani». In considerazione di ciò, la Corte sposa una lettura sufficientemente ampia della nozione di "decisione", di guisa da poter «includere diversi atti che possono incidere sulla persona interessata in vari modi» (punto 46).

Questo passaggio argomentativo viene raggiunto sulla base dell'analisi della disciplina contenuta nel Gdpr e, volgendo l'indagine al caso concreto, la Corte giunge ad affermare che «il risultato del calcolo della solvibilità di una persona sotto forma di tasso di probabilità relativo alla capacità di tale persona di onorare impegni di pagamento in futuro» rappresenta espressione di un momento decisionale (punto 46). Questa prima conclusione

è di fondamentale importanza per comprendere l'impianto argomentativo della Corte e per individuare, in chiave prospettica, ulteriori riflessi della sentenza. Essa consente di mettere in luce che l'elaborazione dell'algoritmo di *scoring* non si riduce ad una mera raccolta di informazioni, riguardanti dati e aspetti personali, assunti da svariate fonti (pubbliche e private), che, opportunamente analizzate e computate, portano a disvelare l'attitudine comportamentale di una persona, bensì appartiene essa stessa al *genus* delle decisioni. D'altronde, nella progettazione degli algoritmi la modellazione prende avvio con la scelta degli obiettivi e in tal senso potremmo dire che gli algoritmi sono ideologicamente orientati, secondo target di efficienza in linea con gli interessi di sviluppatori e progettisti piuttosto che di giustizia, equità o di interesse della comunità²⁴. Peraltro, occorre considerare che essi non riflettono in modo incorrotto la realtà anzi, essendo progettati allo scopo di ottenere determinati risultati attesi, si fondano su una predeterminata rappresentazione della realtà, sotto forma di problemi da risolvere, di variabili incidenti e di parametri opportunamente categorizzati²⁵. Tanto ci consente di argomentare, in via generale, che l'atto decisionale può assumere anche la veste formale dell'algoritmo di *scoring* ed è facile intuire come tale prospettiva verrà ad incidere sulla ripartizione della responsabilità delle organizzazioni coinvolte. Basti solo pensare alle differenti posizioni che esse dovranno assumere, a seconda del caso specifico, con riferimenti ai ruoli definiti dal Gdpr.

Restano da indagare gli ulteriori parametri normativi, quelli che la norma indica come elementi discriminanti tra cosa è vietato, perché rientrando nelle tutele dell'art. 22, e cosa non lo è per la mancanza del fattore "unicamente automatizzato" oppure dell'efficacia rilevante della decisione.

La *ratio* della norma è di stabilire più forti tutele del diritto alla protezione dei dati personali qualora sia presente una stretta correlazione tra il trattamento automatizzato di informazioni personali ed

di divulgare le diverse informazioni utilizzate ai fini di tale calcolo nonché il metodo utilizzato per la loro ponderazione.

23. BINNS-VEALE 2021, p. 321 ss.

24. Osserva BORRUSO 1978, p. 30, che il computer, potendo svolgere le funzioni più diverse, «può servire a tutto come a niente, nella misura in cui è stato istruito».

25. AMATO MANGIAMELI 2019, p. 109.

«effetti giuridici» o esiti significativi sulla persona, tale da poter giudicare questi ultimi come frutto diretto ed esclusivo del primo. Questa forte connessione suggerisce che l'atto decisionale sia direttamente influenzato e guidato dalle operazioni di calcolo automatizzato delle informazioni personali, ciò che la norma mira a contenere. L'incremento di tutela si realizza altresì con un'estensione degli oneri informativi riguardo a informazioni supplementari rispetto a quelle ordinarie (art. 13, par. 2, lett. f, Gdpr) e del diritto di accesso dell'interessato (art. 15, par. 1, lettera h, Gdpr).

Sul punto la Corte si giova, per un verso, del concetto di profilazione ex art. 4, par. 4, Gdpr, che lo stesso legislatore ha classificato nella categoria delle decisioni basate “unicamente sul trattamento automatizzato” (art. 22, par. 1, Gdpr); per altro verso, sugli accertamenti di fatto del giudice del rinvio, da cui risulta che in caso di domanda di mutuo rivolta da un consumatore a una banca, un tasso di probabilità insufficiente comporta, in quasi tutti i casi, il rifiuto di quest'ultima di concedere il prestito richiesto. Questo punto assume particolare rilievo nella prospettiva di analisi che si intende seguire poiché fonda l'interpretazione espansiva della nozione giuridica di “decisione automatizzata”, necessaria per valutare il contesto specifico caratterizzato da una pluralità di agenti. La Corte rileva come l'azione del terzo, al quale è trasmesso il tasso di *scoring*, è guidata da tale tasso in maniera decisiva: «the action of the third party to whom the probability value is transmitted draws 'strongly' on that value». Un accertamento di fatto cui segue un'interpretazione della norma che ha riflessi rilevanti su una serie di questioni fondamentali legate alla tutela dei dati personali, alla certezza del diritto, alle dinamiche del potere decisionale e alla ripartizione della relativa responsabilità.

4. I riflessi della sentenza sulla tutela delle libertà fondamentali

L'analisi sopra riportata consente alcune osservazioni che all'evidenza non possono essere, né pretendono di esserlo, conclusive. Preliminarmente, occorre rilevare che i riflessi della sentenza si estendono al di là del contesto specifico degli algoritmi di *scoring* per l'accesso al credito, riguardando

tutte quelle decisioni basate su una vasta gamma di dati e processi di calcolo complessi, laddove l'atto computazionale influenza la decisione finale grazie a una delega decisionale “strong”. Condizioni che, considerata la complessità sempre più forte delle interazioni tra fattori automatizzati e umani, saranno sempre più diffuse.

Negli algoritmi di *scoring* questa forte connessione tra decisione e trattamento automatizzato di aspetti personali è resa evidente grazie al concetto della profilazione, come positivizzato dall'art. 4, par. 4, Gdpr. Tali strumenti si giovano di un'analisi comportamentale pregressa dell'individuo, basata sulla raccolta massiccia di dati e aspetti personali che poi vengono catalogati, ne viene fatta una classificazione sulla base di classi predefinite al fine di prevedere il comportamento del singolo. La prevedibilità del comportamento individuale discende dall'aver catalogato un individuo entro una classe di propri simili che, sul piano comportamentale, agiscono in modo uniforme tra loro.

La loro legittimità non è posta in discussione. Non dal Gdpr che definisce l'attività di profilazione una forma di trattamento automatizzato dei dati personali «... per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica» (art. 4, lett. 4), che richiederà l'attuazione delle specifiche garanzie di protezione dei dati personali. Il fattore predittivo si riferisce alla capacità di utilizzare i dati raccolti per fare previsioni accurate sul comportamento futuro delle persone, come ad esempio gli acquisti online, le preferenze politiche, le attività criminali o le possibili minacce informatiche. Il fattore predittivo è essenziale perché consente di adottare misure preventive o correttive in anticipo, basandosi sulle informazioni ricavate dalla profilazione. Lo stesso Gdpr ne individua un possibile impiego «a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale» rimettendo al singolo Stato membro l'attuazione e implementazione di regole a garanzia della sicurezza e dell'affidabilità di un siffatto servizio.

E anche l'AI Act²⁶, per certi versi, ne legittima l'utilizzo. Il regolamento prevede di classificare i sistemi di AI in differenti livelli di rischio, secondo una metodologia *risk based*, di guisa da applicare a ciascun livello di rischio un set di strumenti e azioni ad hoc. In particolare, vengono previsti quattro diversi livelli di rischio: rischio inaccettabile, rischio elevato, rischio limitato e rischio minimo. I sistemi di intelligenza artificiale che comportano rischi inaccettabili rappresentano una chiara minaccia per la vita e la sicurezza delle persone, per cui verranno vietati. Per gli altri livelli di rischio sono previsti obblighi via via meno stringenti²⁷.

Per quanto concerne, in particolare, gli strumenti di *scoring* l'AI Act li classifica di rischio inaccettabile qualora ricorrano determinate condizioni. Vieta, ad esempio, l'utilizzo di sistemi che classifichino le «persone fisiche o i gruppi di persone fisiche sulla base di vari punti di dati riguardanti il loro comportamento sociale in molteplici contesti o di caratteristiche personali o della personalità...» qualora il punteggio ottenuto «può determinare un trattamento pregiudizievole o sfavorevole di persone fisiche o di interi gruppi in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti, o a un trattamento pregiudizievole che risulta ingiustificato o sproporzionato rispetto alla gravità del loro comportamento sociale» (c. 31 e art. 5, punto 1, lett. c). Vietato, ancora, è «l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di un sistema di IA per effettuare valutazioni del rischio relative a persone fisiche al fine di valutare o prevedere la probabilità che una persona fisica commetta un reato, unicamente sulla base della profilazione di una persona fisica o della valutazione dei tratti e delle caratteristiche della personalità; tale divieto non si applica ai sistemi di IA utilizzati

a sostegno della valutazione umana...» (art. 5, punto 1, lett. d)

Non sono vietati, invece, poiché classificati tra i sistemi di AI "ad alto rischio" (art. 6, punto 5) quelli destinati a consentire l'accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e fruizione degli stessi, se utilizzati « a) ... dalle autorità pubbliche o per conto di autorità pubbliche per valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica essenziali, compresi i servizi di assistenza sanitaria, nonché per concedere, ridurre, revocare o recuperare tali prestazioni e servizi; b) ... per valutare l'affidabilità creditizia delle persone fisiche o per stabilire il loro merito di credito».

V'è da notare, infine, che non ci sarà una sovrapposizione dell'AI Act rispetto al Gdpr e la materia delle decisioni automatizzate resterà disciplinata dall'art. 22 Gdpr, con il portato di conseguenze e questioni scaturenti dalla sua formulazione. In altri termini, il nuovo contesto normativo rappresentato dall'AI Act non offre delle risposte tecnico-giuridiche alla problematica qui esaminata, né sposta i termini della relativa questione. Ma, sia detto a evitare equivoci, non si tratta di un vuoto normativo, posto che l'AI Act non vuole disciplinare l'intera materia dell'intelligenza artificiale, come una *summa* di tutte le norme, ma vuole soltanto determinare condizioni e requisiti che i sistemi di AI devono rispettare per poter accedere al mercato unico digitale.

Verificata, alla stregua del quadro normativo citato, la legittimità della delega computo-decisionale possiamo attenderci un largo ricorso a tale ausilio, soprattutto nella sua variante "strong". L'ampia diffusione di una delega "strong" deriva, probabilmente, dall'alibi dell'imparzialità²⁸ e dell'oggettività²⁹ del calcolo computazionale – di cui non siamo

26. Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) [AI Act].

27. Cfr. FINOCCHIARO 2022, p. 1085 ss., secondo la quale, mentre il sistema *risk management* è accompagnato dal principio di *accountability* nel GDPR, ciò non accade nell'AI Act, ove la valutazione del rischio dei sistemi intelligenti non è rimessa alle scelte degli operatori economici, ma al legislatore.

28. BORRUSO 1997, par. 13. L'autore afferma che «il computer, a differenza dell'uomo, non si stanca, non dimentica, non si emoziona, non si distrae e, nel rispetto delle distinzioni operate nel programma, è imparziale».

29. «In molti campi gli algoritmi promettono di diventare lo strumento attraverso il quale correggere le storture e le imperfezioni che caratterizzano tipicamente i processi cognitivi e le scelte compiute dagli esseri umani, messi in

ancora sobri – oppure da un'*accountability* delle organizzazioni incapaci di affrancarsi dal potere derivante dalle decisioni automatizzate, oppure dal comandamento dell'efficienza che è ragione e conseguenza della tendenza a narrare di una intelligenza della macchina piuttosto che della macchina intelligente; oppure, ancora, discende da tutti questi fattori assieme. L'efficienza è la ragione più immediata per affidare alcune attività a sistemi automatizzati, capaci di elaborazione dati su larga scala, a velocità non umana, con volumi e aspettative di tassi di errore inferiori rispetto agli esseri umani, con capacità di individuare correlazioni, rapporti, inferenze che nessuna valutazione umana sarebbe in grado di rilevare. E, in chiave prospettica, possiamo pensare che gli sviluppi esponenziali delle capacità computazionali e inferenziali delle nuove tecnologie non freneranno la corsa alla delega compu-decisionale, anzi, saranno sempre più indispensabili per l'uomo³⁰.

A fronte di tale scenario, in contesti molto complessi, fatti di reti di input, algoritmi, dati e influenze umane, sarà sempre più arduo esplorare il rapporto tra atto decisionale ed elaborazione automatizzata di aspetti personali, al fine di indagare la prevalenza dell'uno o dell'altro e, quindi, per poter dare applicazione alle tutele previste dall'art. 22 Gdpr. E, nonostante gli sforzi interpretativi come pure evidenti nella sentenza in rassegna, l'effettività delle tutele per le libertà fondamentali resterà confinata in un perimetro sfuggente.

5. Conclusioni

Le decisioni automatizzate sono sempre più integrate nelle nostre vite quotidiane e lo saranno ancor di più man mano che la tecnologia continuerà ad evolversi. Esse rappresentano una tappa significativa nell'evoluzione degli strumenti

digitali e delle pratiche decisionali per cui diventa essenziale comprendere le implicazioni che ciò comporta e le possibili conseguenze sulla tutela dei diritti fondamentali.

Un primo passo è quello di adottare una prospettiva omnicomprensiva, nel senso di analizzare il fenomeno delle decisioni automatizzate come un "sistema decisionale". Ciò indurrà a valutare le decisioni automatizzate come il frutto di un complesso di interazioni tra differenti componenti, umane e digitali, volgendo così lo sguardo al percorso, al contesto, alle componenti e alle dinamiche del decidere. Nel loro insieme. Lo sguardo unitario saprà includere non solo il momento in cui l'algoritmo viene concepito e addestrato ma anche il contesto in cui viene implementato e le interazioni con le componenti non digitali, quindi, con il soggetto al quale viene imputata la decisione finale.

Analizzare il fenomeno come sistema offre una prospettiva ricca e multidimensionale che può aiutare a comprendere meglio le loro implicazioni: anzitutto, il potere decisionale nell'ambito del "sistema decisionale" resta confinato dove si produce automazione, dacché la capacità di aggregare, elaborare e inferire enormi quantità di dati, quindi di decidere, è un primato della macchina; i decisori umani possono trovarsi in una posizione di dipendenza o subordinazione rispetto alle decisioni generate dalle macchine, residuandone una loro ridottissima – e forse trascurabile – autonomia decisionale³¹; col tempo la capacità di discernimento umana potrebbe ridursi a fronte dell'egemonica efficienza statistico-computazionale; inoltre, la responsabilità resta attribuita formalmente a decisori sforniti del relativo potere decisionale, creando un divario tra chi ha il potere decisionale effettivo e chi ne ha la responsabilità formale, con evidenti conseguenze sull'effettività

luce soprattutto negli ultimi anni da un'imponente letteratura di economia comportamentale e psicologia cognitiva. In tale contesto, le decisioni prese dall'algoritmo assumono così un'aura di neutralità, frutto di asettici calcoli razionali basati su dati», Cons. Stato, Sez. VI, 13 dicembre 2019, n. 8472.

30. Il rapporto annuale della Stanford University, *The AI Index 2024 Annual Report*, dell'AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, dell'aprile 2024, stima che l'intelligenza artificiale ha superato le prestazioni umane in diversi parametri, inclusi alcuni nella classificazione delle immagini, nel ragionamento visivo e nella comprensione dell'inglese. Eppure, resta indietro su compiti più complessi come la matematica a livello competitivo, il ragionamento visivo basato sul buon senso e la pianificazione.

31. MALGIERI-COMANDÉ 2017.

delle tutele previste dall'art. 22 Gdpr³²; infine, indagare la complessità delle diverse dinamiche e interconnessioni che caratterizzano i sistemi decisionali automatizzati, e quindi l'applicabilità delle tutele previste dall'art. 22 Gdpr, potrebbe non esser alla portata di chi, di quelle tutele, ha diritto.

A fronte di tale scenario sarebbe di certo auspicabile che il legislatore si soffermasse, anche per ragioni di certezza del diritto, sui limiti applicativi della nozione positiva di decisione automatizzata, superando l'elemento scriminante della decisione "unicamente automatizzata", foriera di complessità interpretative e difficoltà applicative. Ma non sarebbe sufficiente. Oggi non possiamo non riconoscere alle nuove tecnologie il compito di espandere i confini della cognizione umana, determinando la liberazione della persona dai propri limiti cognitivi e assicurando alla società intera una profonda innovazione³³. E non possiamo rinunciare a tanto. Occorre, quindi, sviluppare una riflessione di sistema sulle ragioni che dovrebbero fondare il ricorso alla delega computazionale e su quelle che, invece, dovrebbero spingere a preservare una decisione umana.

Resta da chiedersi, in altri termini, quanta parte di libertà siamo disposti a cedere e per quale imperativa ragione. Se lo scopo sarà quello di prevenire le frodi o l'evasione fiscale, attacchi terroristici o cyber attacchi, oppure di migliorare le diagnosi mediche e i piani di trattamento sanitario saremo ben disposti a rinunciare ad una parte di libertà. Se lo scopo è quello di dirci ciò che possiamo fare (aprire un mutuo, fittare casa, avere un lavoro ecc.) e, quindi, ciò che possiamo essere, allora ci rendiamo conto di come l'algoritmo predittivo del comportamento umano confini la persona nel proprio vissuto, leghi il suo futuro al suo passato, senza il riconoscimento di un diritto all'oblio comportamentale³⁴.

Le ragioni ideali che portano al riconoscimento di questo interesse all'oblio comportamentale risiedono nel valore della persona umana, caposaldo irrinunciabile del costituzionalismo moderno, tanto nella sua dimensione nazionale che sovranazionale, ed in particolare in quella europea³⁵. In coerenza al principio "personalistico" che informa l'intera Costituzione, l'art. 2 nel riconoscere i diritti

32. CHIODO 2022, pp 39-48, in cui l'autrice esplora il passaggio dalla definizione delle tecnologie in termini di automazione, alla definizione delle tecnologie in termini di autonomia come un cambiamento che «may mean that we are using technologies, and in particular emerging algorithmic technologies, as *scapegoats that bear responsibility for us by making decisions for us*».

33. La visione protetica venne teorizzata almeno un ventennio fa da FROSINI 1998, p. 58, il quale evidenziava come l'informatica avesse determinato una vera mutazione antropologica: «Dialogare attraverso le macchine, o con le macchine stesse, non è la stessa cosa di conversare a viva voce: si adopera una protesi intellettuale, che modifica il procedimento del conoscere e del comunicare. L'uomo è divenuto essenzialmente diverso da quello che è stato in tutti i tempi, e non potrebbe tornare indietro senza perdere la sua nuova umanità, che gli è stata conferita dalla cultura informatica di massa».

34. La prospettiva che si vuol offrire prescinde dalla questione dell'esattezza o meno del contenuto del dato personale e dalla comparazione tra i diritti garantiti dagli artt. 7 e 8 ed il diritto alla libertà di espressione di cui all'art. 11 della Carta dei diritti fondamentali dell'Unione europea. Quanto al diritto all'oblio nella rete si veda MORELLI 2002, p. 851; MARONGIU 2015, pp. 243-264; MEZZANOTTE 2009; MANTELERO 2014, p. 688.

35. In particolare, la Carta dei diritti fondamentali dell'Unione europea contempla il diritto all'integrità della persona, dal quale discende anche quello al consenso libero e informato (art. 3); il diritto alla sicurezza (art. 6); il rispetto alla vita privata e familiare (art. 7); il diritto alla protezione dei propri dati personali (art. 8); il diritto a ricevere informazioni (art. 11.1); il diritto a misure che prevedano vantaggi specifici a favore del sesso sottorappresentato (art. 23); i diritti del bambino (art. 24); i diritti degli anziani (art. 25); i diritti dei disabili (art. 26); per citarne solo alcuni.

inviolabili dell'uomo³⁶ «esalta la persona, assunta come il fondamento e il fine dell'ordine»³⁷.

Non si propone, dunque, una lettura soltanto in termini di pericolo di discriminazione nell'uso dei sistemi decisionali automatizzati, sarebbe riduttivo³⁸. Non si tratta dell'esigenza di tutela di gruppi marginali o minoritari, bensì di tutelare tutti valorizzando le differenze, in quanto necessarie per garantire il pluralismo, la pari dignità sociale (art. 3, comma 1, Cost.), il perseguimento dell'uguaglianza (art. 3, comma 1, Cost.) e il pieno sviluppo della persona umana (art. 3, comma 2, Cost.). La connessione con l'art. 3, comma 2, Cost. è essenziale poiché dopo aver sancito l'uguaglianza dei cittadini di fronte alla legge, indipendentemente da sesso, razza, lingua, opinioni politiche, religiose o sociali, esige che siano rimossi «gli ostacoli di ordine economico e sociale, che (...) impediscono

il pieno sviluppo della persona umana». E in un'epoca in cui l'accesso a molti servizi, sia pubblici che privati, è disposto sulla base di sistemi decisionali automatizzati la cui sofisticazione rende deboli le tutele normative, tali sistemi possono divenire un ostacolo all'affermazione della propria identità, cioè del «diritto di essere sé stesso»³⁹.

Nel mondo digitale viene a mancare alla persona quella tutela *naturaliter* dello scorrere del tempo, fondamento basilare dell'oblio. Tutela che va reintegrata con i necessari aggiustamenti. Non che debbano introdursi altri diritti. L'idea di fondo è che i «sistemi decisionali automatizzati» debbano esser permeati da una prospettiva incentrata sui diritti fondamentali⁴⁰, sì da bilanciare uno sviluppo orientato esclusivamente all'efficienza delle nuove tecnologie.

Riferimenti bibliografici

- A.C. AMATO MANGIAMELI (2023), *Intelligenza artificiale. Origine e principi*, in A.C. Amato Mangiameli, G. Saraceni (a cura di), «Cento e una voce di informatica giuridica», Giappichelli, 2023
- A.C. AMATO MANGIAMELI (2019), *Algoritmi e big data. Dalla carta sulla robotica*, in «Rivista di filosofia del diritto», 2019, n. 1
- D. AMOROSO, G. TAMBURRINI (2019), *I sistemi robotici ad autonomia crescente tra etica e diritto: quale ruolo per il controllo umano?*, in «BioLaw Journal – Rivista di BioDiritto», 2019, n. 1
- N. APPELMAN, R.Ó FATHAIGH, J. VAN HOBOKEN (2022), *Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands*, in «Journal of Intellectual Property, Information Technology and E-Commerce Law», vol. 12, 2022, n. 4

36. Sul concetto di personalità si registrano due opposti orientamenti: da un lato, esisterebbe un unico diritto della personalità che considera la persona nella sua unitarietà e il diritto all'immagine, al nome, all'onore, alla reputazione, alla riservatezza non sono che singoli aspetti della rilevanza costituzionale, su cui v. GIAMPICCOLO 1958, p. 466; FERRI 1984, p. 137; Cass., 10 maggio 2001, n. 6507, in «La nuova giurisprudenza civile commentata», 2002, n. 1, p. 529; e dall'altro, vi sarebbero tanti diritti della personalità quanti la legge ne preveda o il giudice ne individui sulla base del tessuto sociale e giuridico, su cui v. DI MAJO 1962, p. 69; Cass., Sez. un., 11 novembre 2008, n. 26973, in «Foro italiano», 2009, n. 1, p. 120.

37. Cfr. COSTA 2008, p. 396; MANGIAMELI 2020, p. 86.

38. I casi di discriminazione operati da sistemi automatizzati sono ben noti, così come le conseguenze sulla vita delle persone che hanno perduto opportunità di lavoro e di istruzione, credito, assistenza sociale e sanitaria. Cfr. APPELMAN-FATHAIGH-VAN HOBOKEN 2022.

39. Corte cost., 3 febbraio 1994, n. 13. Sull'attitudine della dimensione di Internet a minacciare la corretta rappresentazione della stessa identità personale v. MORELLI 2019, p. 49.

40. Molto efficacemente sull'argomento AZZARITI 2022, p. 4, di cui si riporta questo lucido passaggio «È così che l'autore che ha insegnato ai giuristi l'importanza e le virtù delle nuove tecnologie, mai da rigettare, sempre da valorizzare, è anche l'autore che ci avvisa dei rischi di un'utilizzazione della tecnica non conforme a costituzione, governata dal mercato e non posta a garanzia dei diritti fondamentali».

- G. AZZARITI (2022), *Stefano Rodotà e l'uso costituzionalmente orientato delle nuove tecnologie*, in "Costituzionalismo.it", 2022, n. 2
- G. BIFERALI (2018), *Big data e valutazione del merito creditizio per l'accesso al peer to peer lending*, in "Diritto dell'informazione e dell'informatica", 2018, n. 3
- R. BINNS, M. VEALE (2021), *Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR*, in "International Data Privacy Law", vol. 11, 2021, n. 4
- R. BORRUSO (1997), *Informatica giuridica*, in "Enciclopedia del diritto", agg. I, Giuffrè, 1997
- R. BORRUSO (1988), *Computer e diritto*, Giuffrè, 1988
- L.A. BYGRAVE (2001), *Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, in "Computer Law & Security Review", vol. 17, 2001, n. 1
- S. CHIDO (2022), *Human autonomy, technological automation (and reverse)*, in "AI & Society", vol. 37, 2022
- P. COSTA (2008), *Diritti fondamentali*, in "Enciclopedia del diritto", Annali, II, Giuffrè, 2008
- A. DI MAJO (1962), *Profili dei diritti della personalità*, in "Rivista trimestrale di diritto e procedura civile", 1962
- G. FASANO (2020), *L'intelligenza artificiale nella cura dell'interesse generale*, in "Giornale di Diritto Amministrativo", 2020, n. 6
- G.B. FERRI (1984), *Oggetto del diritto della personalità e danno non patrimoniale*, in "Rivista del diritto commerciale e del diritto generale delle obbligazioni", 1984, n. 1-4
- G. FINOCCHIARO (2022), *La regolazione dell'intelligenza artificiale*, in "Rivista trimestrale di diritto pubblico", 2022, n. 4
- V. FROSINI (1998), *Il giurista e le tecnologie dell'informazione*, Bulzoni Editore, 1998
- D.-U. GALETTA, J.G. CORVALÁN (2019), *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *Federalismi.it*, 2019, n. 3
- G. GIAMPICCOLO (1958), *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza*, in "Rivista trimestrale di diritto e procedura civile", 1958
- GRUPPO DI LAVORO ARTICOLO 29 (2020), *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, 2020
- D. KORFF (2002), *EC study on implementation of data protection directive. Comparative summary of national laws*, Human Rights Centre, 2002
- E. LONGO (2019), *Dai big data alle «bolle filtro»: nuovi rischi per i sistemi democratici*, in "Percorsi costituzionali", 2019, n. 1
- G. MALGIERI, G. COMANDÉ (2017), *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in "International Data Privacy Law", vol. 7, 2017, n. 3
- S. MANGIAMELI (2020), *I diritti costituzionali: dallo Stato ai processi di integrazione*, Giappichelli, 2020
- A. MANTELERO (2014), *Il futuro regolamento EU sui dati personali e la valenza "politica" del caso Google: ricordare e dimenticare nella digital economy*, in "Il Diritto dell'informazione e dell'informatica", 2014, n. 4-5
- D. MARONGIU (2015), *Il diritto all'oblio come diritto all'esclusione dai motori di ricerca. Dalla giurisprudenza europea al diritto amministrativo italiano*, in "Diritto e processo amministrativo", 2015, n. 1

- M. MEZZANOTTE (2009), *Il diritto all'oblio. Contributo allo studio della privacy storica*, Edizioni Scientifiche Italiane, 2009
- A. MORELLI (2019), *Persona e identità personale*, in "BioLaw Journal – Rivista di BioDiritto", 2019, n. 2
- R. MORELLI (2002), voce *Oblio (diritto all')*, in "Enciclopedia del diritto", agg. IV, Giuffrè, 2002
- OECD (2024), *Explanatory memorandum on the updated OECD definition of an AI system*, OECD Artificial Intelligence Papers, No. 8, OECD Publishing, 2024
- E. PARISIER (2011), *The filter bubble: What the Internet is hiding from you*, Penguin, 2011
- D. PORRINI (2018), *Big data, personalizzazione delle polizze ed effetti nel mercato assicurativo*, in V. Falce, G. Ghidini, G. Olivieri (a cura di), "Informazione e big data tra innovazione e concorrenza", Giuffrè, 2018
- S. RODOTÀ (1995), *Tecnologie e diritti*, il Mulino, 1995
- K. SHAFFER (2019), *Data versus Democracy: How Big Data Algorithms Shape Opinions and Alter the Course of History*, Apress, 2019
- A. SIMONCINI (2019), *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in "BioLaw Journal – Rivista di BioDiritto", 2019, n. 1
- S. WACHTER, B. MITTELSTADT, L. FLORIDI (2017), *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, in "International Data Privacy Law", 2017



PAOLO ZUDDAS

Intelligenza artificiale in medicina: alcune risposte – significative, ma parziali – offerte dal codice di deontologia medica (in materia di non discriminazione, consenso informato e relazione di cura)

L'analisi proposta è tesa a valutare l'impatto prodotto dall'impiego di sistemi di intelligenza artificiale in medicina in relazione ad alcuni profili di primario rilievo nella pratica medica. In particolare, si intende evidenziare come il ricorso a sistemi di AI medica: aumenti il rischio di operare discriminazioni nell'erogazione delle prestazioni sanitarie, in conseguenza dell'impiego, nell'addestramento dei sistemi di *machine learning*, di dati distorti e di dati incompleti; ponga in crisi l'istituto del consenso informato, stante la necessità di fornire informazioni complete concernenti anche le logiche di funzionamento dei sistemi informatici eventualmente coinvolti nell'attività diagnostica o terapeutica, a fronte delle note forme di opacità dei sistemi di AI; trasformi progressivamente il rapporto di cura, con ricadute destinate ad incidere sia sulla natura delle valutazioni cliniche sia sul ruolo del medico, chiamato ad operare sempre più come intermediario tra il paziente e il sistema informatico. Muovendo da queste premesse, sarà valutata l'adequatezza delle soluzioni alle questioni evocate che possono essere offerte dal Codice di deontologia medica attualmente in vigore.

AI medica – Bias – Black-box – Relazione medico-paziente

Artificial intelligence in medicine: some – significant, but partial – answers offered by the code of medical ethics (on non-discrimination, informed consent and the doctor-patient relationship)

This study aims at assessing the impact produced by the use of artificial intelligence systems in medicine in relation to some aspects of primary importance in medical practice. In particular, the object is to highlight how the use of medical AI systems: increases the risk of discriminating in the provision of healthcare services, as a result of the use of biased data and incomplete data in the training of machine learning systems; undermines the informed consent, in view of the need to provide complete information also concerning the decision-making logic of the computer systems that may be involved in the diagnostic or therapeutic activity (all this bearing in mind the well-known forms of opacity of AI systems); progressively transforms the doctor-patient relationship with effects on the nature of clinical evaluations and on the role of the doctor, who is called upon to act increasingly as an intermediary between the patient and the computer system. Starting from these premises, the study will attempt to assess the adequacy of the solutions to the mentioned issues that can be offered by the Code of Medical Ethics currently in force.

Medical AI – Bias – Black-box – Doctor-patient relationship

L'Autore è professore associato di Diritto costituzionale e pubblico presso l'Università dell'Insubria

SOMMARIO: 1. Note introduttive: i benefici e i rischi dell'AI medica e il difficile ruolo del legislatore. – 2. Al medica e principio di non discriminazione: il nesso inscindibile tra qualità – ed equità – delle prestazioni sanitarie e qualità – e completezza – dei dati sanitari utilizzati. – 2.1. *Il caso della c.d. medicina potenziativa: disuguaglianza nell'accesso alle prestazioni sanitarie e impatto sulle "condizioni personali" dei cittadini.* – 3. Al medica e consenso informato: la libertà di cura in bilico tra necessaria comprensibilità dell'informazione richiesta per il consenso e opacità dei sistemi di apprendimento automatico. – 3.1. *I rischi di "corto circuito" legati all'obbligo di illustrare al paziente le logiche di funzionamento dell'intelligenza artificiale.* – 3.2. *Tra consenso informato e relazione di cura: il ruolo dell'informazione (e dell'empatia) nella costruzione del rapporto fiduciario tra medico e assistito.* – 4. Al medica e relazione di cura: la progressiva trasformazione del rapporto medico-paziente in rapporto medico-paziente-intelligenza artificiale. – 4.1. *La centralità della visita medica e il ruolo dei dati nelle valutazioni cliniche.* – 4.2. *Il mutamento del ruolo del medico conseguente alla trasformazione della relazione di cura in un rapporto trilatero.* – 5. Nota conclusiva: il "rispetto della persona umana" come primato dell'uomo sulla macchina?

1. Note introduttive: i benefici e i rischi dell'AI medica e il difficile ruolo del legislatore

Le applicazioni di intelligenza artificiale in medicina costituiscono un aspetto di crescente rilevanza nell'ambito della c.d. *e-health*, cioè dell'uso di tecnologie informatiche e di telecomunicazione a beneficio della salute umana¹: un ambito amplissimo, che si estende dalla c.d. telemedicina – che ricomprende l'insieme degli strumenti che consentono l'acquisizione di dati sanitari e l'erogazione di prestazioni sanitarie "a distanza" – fino alle più avanzate applicazioni della robotica sia in ambito clinico (a supporto dell'attività diagnostica e terapeutica, con un particolare impiego nella

chirurgia), sia in quello riabilitativo e assistenziale (a sostegno degli operatori assistenziali e dei *care-givers*)².

In particolare, l'intelligenza artificiale può essere impiegata a supporto della formulazione sia di ipotesi di diagnosi, sia di proposte di terapia.

Rispetto all'attività diagnostica, gli strumenti informatici attualmente disponibili permettono, tra l'altro, di operare un controllo costante dello stato di salute anche attraverso l'impiego di tecnologie digitali indossabili che monitorano le funzioni vitali, i toni dell'umore e l'attività neuroendocrina³, mentre l'analisi automatizzata delle indagini cliniche può consentire di elaborare modelli di predizione dell'insorgere di una malattia⁴.

1. Si v. in proposito la definizione offerta dall'Organizzazione Mondiale della Sanità, che qualifica l'*e-health* come «the cost-effective and secure use of information and communications technologies in support of health and health-related fields, including health-care services, health surveillance, health literature, and health education, knowledge and research» (cfr. WORLD HEALTH ORGANIZATION 2012).

2. Cfr. sul tema BIANCARDO 2021, p. 111.

3. In argomento v., *ex multis*, MAJUMDER-MONDAL-DEEN 2017

4. Può essere utile richiamare, in proposito, alcune esperienze pratiche: la Carnegie Mellon University ha realizzato un algoritmo di apprendimento automatico capace di analizzare e comparare 72 parametri clinici al fine di comprendere se il paziente esaminato sia predisposto ad avere un infarto, riuscendo a predire il verificarsi

Rispetto all'attività terapeutica, l'intelligenza artificiale è ampiamente coinvolta nella elaborazione delle c.d. terapie digitali (DTx)⁵ ed è in grado di garantire una costante ed efficace assistenza ai pazienti nell'autogestione delle malattie croniche, come ipertensione e diabete. Anche in questo ambito, inoltre, l'AI è utilizzata a fini predittivi, nella elaborazione di modelli di previsione dell'esito clinico delle terapie⁶.

Inoltre, alcune applicazioni di intelligenza artificiale – come ad esempio *Watson* di IBM⁷ – coniugano entrambe le attività e sono quindi in grado di garantire insieme un controllo costante di parametri vitali e la conseguente somministrazione di piani terapeutici, realizzando un'interlocuzione diretta con il paziente. Applicazioni a cui si affianca l'utilizzo di *chatbot* come “medici di famiglia virtuali”⁸, sul modello di *Babylon Health*, un servizio di medicina generale privato sviluppato in Gran Bretagna, erogato attraverso un'app⁹.

Va richiamato, infine, il settore chirurgico, che vede l'intelligenza artificiale applicata sia alla c.d. chirurgia assistita e video assistita, sia alla c.d. chirurgia robotica. In particolare, la prima comporta l'utilizzo di bracci meccanici o di dispositivi simili guidati da un chirurgo attraverso una consolle¹⁰ e può anche permettere di realizzare operazioni in remoto, laddove il chirurgo si trovi in luoghi

diversi da quello in cui opera la macchina controllata: quest'ultimo impiego, peraltro, si protrae ormai da più vent'anni, risalendo al 2001 la prima colecistectomia realizzata da un chirurgo a New York su un paziente a Strasburgo, ed è destinato a perfezionarsi ulteriormente soprattutto a seguito della diffusione della tecnologia 5G, che azzera sostanzialmente l'asincronia tra comandi impartiti e movimenti della macchina¹¹. La chirurgia robotica prevede invece un sistema misto *hardware-software* programmabile, che esegue operazioni complesse. In particolare, l'applicazione crescente dell'intelligenza artificiale alla robotica ha progressivamente innalzato il livello di auto-apprendimento e conseguentemente di autonomia dei sistemi misti impiegati in questo settore¹², generando numerosi interrogativi, che investono tra l'altro: la gestione dei rischi legati ai crescenti margini di imprevedibilità nell'azione delle macchine; i connessi problemi relativi all'imputazione della responsabilità giuridica; la scelta dell'approccio preferibile nell'impostazione del rapporto uomo-macchina (che può riassumersi principalmente nel seguente dilemma: è la macchina che deve correggere gli errori dell'uomo o è l'uomo che deve correggere gli errori della macchina?)¹³.

In ordine agli effetti che gli impieghi delle tecnologie informatiche sono in grado di produrre

dell'evento con una precisione dell'80% (come riportato da *The Economist*, *Of prediction and policy*, 20 agosto 2016); un'équipe di studiosi statunitensi, argentini e brasiliani ha sviluppato un modello di AI che individua tic verbali e schemi ricorrenti nel parlare, utilizzabile per analizzare le trascrizioni dei discorsi dei pazienti, al fine di comprendere chi potrebbe soffrire di psicosi o di schizofrenia (cfr. BEDI-CARRILLO-CECCHI et al. 2015); l'azienda di tecnologia biomedica Medtronic ha elaborato uno strumento di AI, denominato “GI Genius”, che opera come un “osservatore virtuale” nel corso della colonscopia, rendendola più precisa e agevolando il rilevamento del cancro al colon (cfr. AA.VV. 2020). Sul tema cfr., per tutti, CHENXI-DIAN-ZHE 2020.

5. Come, ad esempio, *Insulia* o *Oleena*: in argomento v., per tutti, PHAN-MITRAGOTRI-ZHAO 2023.

6. In tema cfr. ALIPER-KUDRIN-POLYKOVSKIY et al. 2023.

7. Un'ampia raccolta di studi sullo strumento in oggetto è contenuta in KANG YOON-JUNHEWK 2016. Per una valutazione dei risultati operativi, v., per tutti, STRICKLAND 2019.

8. Cfr. sul punto l'analisi promossa dal Consiglio d'Europa contenuta nel documento MITTELSTADT 2021, p. 30.

9. Una sintetica ed efficace descrizione del sistema è contenuta in MALVA-ZURLO 2019.

10. Cfr. BIANCARDO 2021, pp. 103, 105 e 111. In proposito possono ricordarsi, ad esempio: *AESOP*, un braccio robotico guidato dal chirurgo attraverso un comando vocale, e *Da Vinci*, il primo sistema di chirurgia video-assistita attraverso una consolle, seguito poi da *Zeus* (ivi, p. 113).

11. *Ivi*, pp. 113-114.

12. Guang-Zhong Yang, Direttore dell'*Hamlyn Centre for Robotic Surgery*, presso l'Imperial College di Londra, ha individuato ben 6 livelli di autonomia della chirurgia robotica, illustrati in YANG-CAMBIAS-CLEARY et al. 2017.

13. Cfr. BIANCARDO 2021, pp. 119 e 137 ss.

sulla gestione della salute umana, va sottolineato con decisione, prima di soffermarsi nel dettaglio sui numerosi rischi che queste tecnologie comportano, che la digitalizzazione tendenzialmente incrementa e migliora le prestazioni sanitarie, incidendo notevolmente sull'effettività del diritto alla salute come diritto sociale.

In particolare, sotto il profilo quantitativo, le applicazioni dell'intelligenza artificiale alla telemedicina consentono di estendere l'erogazione di prestazioni sanitarie a fasce di popolazione più svantaggiate¹⁴, garantendo l'accesso alle cure in luoghi remoti o inaccessibili o che soffrono di una carenza di operatori sanitari¹⁵. Sotto il profilo qualitativo, oltre alle cennate capacità elaborative e predittive dell'intelligenza artificiale e alle promettenti applicazioni della chirurgia robotica, le nuove tecnologie informatiche garantiranno nel futuro una crescente "personalizzazione" delle cure, contribuendo alla costruzione di un'assistenza sanitaria – come ha osservato l'Organizzazione Mondiale della Sanità – «sempre più incentrata sul paziente, con approcci personalizzati al processo decisionale», che implicheranno un sempre maggiore "coinvolgimento" dell'assistito nelle strategie di cura¹⁶.

Queste innovazioni, tuttavia, presentano altrettanti "lati oscuri": la personalizzazione delle cure, derivante dall'utilizzo crescente di sistemi di apprendimento automatico per elaborare i dati sanitari, impone un maggiore coinvolgimento del paziente anche nella comprensione delle scelte terapeutiche elaborate con l'ausilio di sistemi informatici; la crescente autonomia di tali sistemi e l'affidamento ad essi della gestione diretta della relazione col paziente rischia di condurre a una "disumanizzazione" del rapporto tra assistito e operatore sanitario; la crescente accuratezza delle ipotesi di diagnosi o di terapia proposte dai sistemi automatici dipende dalla natura e dai caratteri delle informazioni acquisite dalla macchina e dunque non avvantaggia tutti i pazienti allo stesso modo,

perché il sistema informatico offre risposte adeguate (o comunque migliori) solo ai pazienti che appartengono alle categorie sulle quali il sistema possiede più informazioni. Questi, in sintesi, alcuni tra i problemi più rilevanti di cui ci si occuperà nella presente analisi, tesa a valutare l'impatto dell'utilizzo dell'intelligenza artificiale in medicina rispetto a tre diversi profili: la non-discriminazione, il consenso informato e la relazione di cura.

Le risposte che il diritto è in grado di offrire alle complesse questioni evocate risentono anzitutto di un limite di carattere generale che va emergendo con sempre maggiore evidenza: se infatti il diritto ha sempre "seguito" lo sviluppo tecnologico – ma mantenendo sempre una certa capacità di prevederne, se non l'evoluzione, perlomeno le applicazioni pratiche più prossime – l'impressione che si ricava dalla lettura delle normative più recenti che si occupano di intelligenza artificiale è che, in questo settore, il diritto si trovi piuttosto a "inseguire" lo sviluppo tecnologico, incatenato in un costante paradosso di Zenone che lo rende incapace di catturare un fenomeno in costante movimento. Un limite che costituisce in realtà un problema drammatico, in quanto la capacità di previsione dei comportamenti umani rappresenta un presupposto essenziale della produzione normativa.

L'approccio originario adottato nel nostro ordinamento (ma anche in sede europea) è stato quello di adattare gli istituti giuridici preesistenti alla disciplina delle nuove tecnologie: questo è avvenuto, ad esempio, con l'applicazione ai robot dotati di sistemi di AI della disciplina in materia di responsabilità per danno da prodotti difettosi (segnatamente nel caso di danni causati direttamente o indirettamente da macchine) e più in generale delle regole sulla sicurezza dei prodotti¹⁷. Appare tuttavia sempre più evidente che alcuni degli istituti giuridici tradizionali, di fronte a sistemi tecnologici dotati di margini sempre più ampi di autonomia, dovranno essere interamente ripensati¹⁸. Da questo punto di vista, l'approccio

14. Cfr. in proposito il recente studio promosso sul tema dall'Organizzazione Mondiale della Sanità: WORLD HEALTH ORGANIZATION 2023, *Foreword*, p. V.

15. Cfr. sul punto MITTELSTADT 2021, p. 44.

16. WORLD HEALTH ORGANIZATION 2023, p. 4.

17. Cfr. sul tema BIANCARDO 2021, pp. 104 e 131 ss.

18. In argomento cfr. ad es. BIANCARDO 2018, p. 109 ss.

adottato dall'Unione europea attraverso l'*Artificial Intelligence Act*, che propone una disciplina dell'intelligenza artificiale modulata su diversi livelli di rischio rispetto alla tutela di alcuni valori giuridici fondamentali, può rivelarsi molto utile, perché incentra la regolamentazione – più che sulle specifiche modalità di funzionamento delle macchine (che sono e presumibilmente saranno sempre più complesse e, per così dire, “sfuggenti”, per tornare alla metafora dell'inseguimento) – sul loro impatto rispetto a principi e valori propri dell'essere umano e sulle responsabilità dell'uomo sia in quanto utilizzatore sia in quanto produttore.

Ciò premesso, l'analisi proposta di seguito intende incentrarsi in particolare sulla disciplina offerta dal codice di deontologia medica attualmente in vigore¹⁹, che include anche alcune norme specificamente riferite all'uso della tecnologia informatica in sanità, contenute principalmente nell'art. 78 e nei relativi indirizzi applicativi; le norme deontologiche saranno inoltre poste a confronto con la disciplina dettata dalla Carta europea di etica medica²⁰.

Tuttavia, non potranno – naturalmente – essere trascurati i principi e i valori contenuti in atti normativi di rango superiore, come la Convenzione europea dei diritti dell'uomo e la Carta dei diritti fondamentali dell'Unione europea e, anzitutto, la nostra Costituzione, che offre ai principi deontologici che richiameremo un fondamento giuridico particolarmente solido. Segnatamente, trovano un

chiaro fondamento nella Costituzione italiana tutti e tre i principi e gli istituti in relazione ai quali si intende valutare l'impatto dell'intelligenza artificiale in medicina: il principio di non discriminazione trova espressione nel primo comma dell'art. 3 Cost., che sancisce l'eguaglianza di fronte alla legge «senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali»; il consenso informato è espressione del principio di “libertà di cura” sancito dal secondo comma dell'art. 32 Cost.; la relazione di cura trova un solido fondamento costituzionale nel necessario «rispetto della persona umana» anch'esso sancito dal secondo comma dall'art. 32 Cost.²¹.

Se la Costituzione non richiama espressamente nessuno degli istituti evocati (per quanto il principio di non discriminazione si desuma molto chiaramente dal secondo comma dell'art. 3 al di là del tenore letterale della disposizione), la Carta dei diritti fondamentali dell'Unione europea²² contiene dei riferimenti più espliciti, citando testualmente sia il principio di non discriminazione (art. 21) sia il consenso informato (art. 3, par. 2).

Disposizioni specificamente dedicate alla pratica medica – che costituiscono un utile elemento di confronto con la disciplina dettata dal codice deontologico – si trovano invece all'interno della Convenzione europea dei diritti dell'uomo, prima evocata, e soprattutto nella Convenzione di Oviedo, che costituisce il più importante documento prodotto dal Consiglio d'Europa in materia²³.

19. *Codice di deontologia medica*, approvato a Torino il 18 maggio 2014 e sottoposto successivamente alle seguenti modifiche: art. 54 modificato in data 16 dicembre 2016; art. 56 modificato in data 19 maggio 2016; art. 76 modificato in data 15 dicembre 2017; art. 76-bis, inserito in data 15 dicembre 2017; art. 17 integrato da indirizzi applicativi “Atti finalizzati alla morte” il 6 febbraio 2020.

20. Il testo della *Carta europea di etica medica*, approvata a Kos (l'isola greca in cui nacque Ippocrate) l'11 giugno 2011, è pubblicato in calce al *Codice di deontologia medica*, pp. 45 ss.

21. Per una ricostruzione della dimensione costituzionale del diritto alla salute v., per tutti, MORANA 2021.

22. Adottata a Nizza il 7 dicembre 2000 e modificata a Strasburgo nel 2007, la *Carta*, dal 2009, costituisce fonte del diritto dell'Unione europea dotata «dello stesso valore giuridico dei trattati» istitutivi (cfr. art. 6 TUE).

23. Si tratta, per la precisione, della *Convenzione europea per la protezione dei diritti dell'uomo e della dignità dell'essere umano riguardo alle applicazioni della biologia e della medicina* (STE n. 164) adottata dal Consiglio d'Europa e siglata ad Oviedo il 4 aprile 1997. In proposito, va tuttavia ricordato che, a dispetto della rilevanza, l'efficacia normativa dell'atto è assai dubbia: la Convenzione, infatti, è stata resa esecutiva dall'Italia con la legge di autorizzazione alla ratifica n. 145 del 2001, ma i suoi effetti si produrranno solo a seguito del deposito dello strumento di ratifica presso il Consiglio d'Europa (in base a quanto previsto sia dall'art. 33 della Convenzione, sia dall'art. 2 della legge 145/2001). Ad oggi, tuttavia, tale deposito non è ancora avvenuto e dunque la Convenzione, formalmente, nel nostro ordinamento è ancora priva di vigenza (in argomento, si v., per tutti, PENASA 2007).

Ampi riferimenti alla tematica sono presenti, naturalmente, anche all'interno della legislazione ordinaria.

Va ricordato, infine, che il ruolo dell'intelligenza artificiale in medicina da diversi anni forma oggetto di una riflessione in seno all'Organizzazione Mondiale della Sanità, che ha recentemente costituito, in collaborazione con l'ITU (Unione internazionale delle telecomunicazioni), un *Focus Group* sulla "AI per la salute"²⁴, articolato in sei sottogruppi, che si occupano, tra l'altro, di "documentazione e trasparenza" (area tematica 1), e di "qualità dei dati" (area tematica 4)²⁵: temi che, come vedremo, rivestono un particolare interesse ai fini della presente analisi.

2. Al medica e principio di non discriminazione: il nesso inscindibile tra qualità – ed equità – delle prestazioni sanitarie e qualità – e completezza – dei dati sanitari utilizzati

Il codice deontologico declina il principio di non discriminazione rispetto a due diversi profili: non discriminazione nell'accesso alle cure e non discriminazione nell'esercizio dell'attività di cura (il che comporta, in ultima analisi, l'obbligo di non differenziare la *qualità* delle prestazioni erogate a danno di specifiche categorie, che sono di norma le categorie protette dal ricordato art. 3 della Costituzione).

In ordine al primo profilo, va richiamato l'art. 6 del codice di deontologia medica (*Qualità professionale e gestionale*), che, al secondo comma, stabilisce che «il medico, in ogni ambito operativo, persegue l'uso ottimale delle risorse pubbliche e private [...] contrastando ogni forma di discriminazione nell'accesso alle cure». Questa prospettiva, che concentra l'attenzione su una condizione preliminare rispetto al concreto svolgimento dell'attività di cura e alle modalità del suo esercizio, corrisponde all'impostazione tradizionale accolta

dalla Costituzione italiana, che postula anzitutto l'accesso alle cure in condizioni di eguaglianza²⁶.

In ordine al secondo profilo, l'art. 3 del codice deontologico (*Doveri generali e competenze del medico*) qualifica l'obbligo di non discriminare nello svolgimento dell'attività di cura (in senso lato) come un vero e proprio "dovere" del medico, affermando che «doveri del medico sono la tutela della vita, della salute psico-fisica, il trattamento del dolore e il sollievo della sofferenza, nel rispetto della libertà e della dignità della persona» (due profili che torneranno in rilievo più avanti, con riguardo rispettivamente al consenso informato ed alla relazione di cura) «senza discriminazione alcuna, quali che siano le condizioni istituzionali o sociali nelle quali opera».

In particolare, merita una specifica sottolineatura il richiamo conclusivo, che ribadisce il dovere del medico di non discriminare anche in base alle «condizioni [...] sociali» dei pazienti. Tale precisazione riveste infatti un peculiare rilievo sotto il profilo costituzionale in quanto la formula "condizioni sociali" compare nel primo comma dell'art. 3 Cost. tra gli elementi in base ai quali si ribadisce il divieto di operare discriminazioni, ma trova riscontro anche nel comma successivo, che impegna la Repubblica a intervenire per rimuovere gli ostacoli di ordine economico e, per l'appunto, "sociale" che limitano "di fatto" l'eguaglianza di cittadini: la formula in oggetto, pertanto, costituisce un "ponte" tra i due commi dell'art. 3 Cost. e collega insieme l'eguaglianza formale, sancita dal primo comma, e l'eguaglianza sostanziale del secondo comma, ribadendo che non solo i consociati non devono essere discriminati in conseguenza della fragilità della propria condizione sociale, ma tale condizione di debolezza sociale deve essere annullata (o, perlomeno, attenuata) a seguito dell'intervento dei pubblici poteri²⁷. Quest'ultimo impegno coinvolge in parte anche il medico, chiamato a svolgere un'opera di tutela nei confronti dei "soggetti fragili" (anche) sul piano sociale, a

24. WORLD HEALTH ORGANIZATION 2023, *Foreword*, p. V: si tratta del *Focus Group on AI for Health* (FG-AI4H).

25. *Ivi*, p. 6.

26. In particolare, il principio di non discriminazione nell'accesso alle prestazioni sanitarie riguarda sia le prestazioni individuali, sia le c.d. prestazioni indivisibili – cioè rivolte alle generalità dei consociati – che caratterizzano il profilo "oggettivo" della salute come "interesse della collettività" (come, ad esempio, le prestazioni di prevenzione delle malattie diffuse ed alcuni interventi nel campo dell'igiene): sul punto cfr. MORANA 2021, p. 3.

27. Sul punto sia consentito rinviare a ZUDDAS 2019, p. 112 ss.

combattere le situazioni di degrado sociale che si sviluppano all'interno di ambienti di vita inidonei a proteggere non solo la salute ma anche la dignità delle persone e a denunciare all'autorità pubblica le situazioni di discriminazione (anche) sociale: un impegno sancito espressamente dal codice deontologico all'art. 32 (*Doveri del medico nei confronti dei soggetti fragili*), a mente del quale «il medico tutela il minore, la vittima di qualsiasi abuso o violenza e la persona in condizioni di vulnerabilità o *fragilità* psico-fisica, *sociale* o civile in particolare quando ritiene che l'*ambiente* in cui vive non sia idoneo a proteggere la sua salute, la dignità e la qualità della vita. Il medico *segnala all'Autorità competente le condizioni di discriminazione*, maltrattamento fisico o psichico, violenza o abuso sessuale».

Il principio di non discriminazione risulta formulato in termini sostanzialmente analoghi nella Carta europea di etica medica, che, nell'individuare un breve elenco di "Principi etici", lo inserisce in esordio alla disciplina, stabilendo al *Principio 1* che «il medico difende la salute fisica e psichica dell'uomo, dà sollievo dalle sofferenze nel rispetto della vita e della dignità della persona, *senza alcun tipo di discriminazione*, di qualunque natura essa sia, in tempo di pace come in tempo di guerra». In aggiunta, la Carta dedica specificamente alla non discriminazione il successivo *Principio 3*, ribadendo che «il medico, *senza discriminazione alcuna*, fornisce al paziente le cure più essenziali ed appropriate».

La distinzione tra i due profili rispetto ai quali può declinarsi il principio in parola – che vieta pertanto trattamenti differenziati irragionevoli sia nell'accesso sia nella qualità dei servizi sanitari erogati – riflette l'impostazione che caratterizza, come prima anticipato, uno degli atti normativi di livello sovranazionale più rilevanti in ambito medico quale è la Convenzione di Oviedo. In particolare,

l'art. 3 della Convenzione – richiamando espressamente i due profili evocati – prescrive un *accesso* equo all'assistenza sanitaria di *qualità* adeguata: ne consegue che la disuguaglianza nell'accesso alle cure o negli standard di cura va considerata una violazione dell'art. 14 della Convenzione europea dei diritti dell'uomo, che sancisce espressamente il divieto di discriminazioni, «in particolare quelle fondate sul sesso, la razza, il colore, la lingua, la religione, le opinioni politiche o quelle di altro genere, l'origine nazionale o sociale, l'appartenenza a una minoranza nazionale, la ricchezza, la nascita od ogni altra condizione»²⁸.

La medesima distinzione si trova riproposta all'interno della disciplina che il codice deontologico dedica all'utilizzo delle tecnologie informatiche in ambito medico. In particolare, tra le "precauzioni e prescrizioni" rivolte al medico nell'utilizzo di «strumenti derivanti dall'uso di tecnologie di informazione e comunicazione di dati clinici» che formano oggetto degli *Indirizzi applicativi* dell'art. 78 (*Tecnologie informatiche*), compare (*sub 2*) l'obbligo di «collabora[re] a eliminare ogni forma di *discriminazione* nell'uso delle tecnologie informatiche e a garantire uguaglianza nell'*accesso* e nell'utilizzo dei servizi sanitari».

Può essere utile, tuttavia, interrogarsi su quale tra i due profili – disuguaglianza nell'accesso alle cure o disuguaglianza nella qualità delle cure – appaia maggiormente interessato dal ricorso alle nuove tecnologie. Da questo punto di vista, pur risultando – come vedremo – coinvolti entrambi i profili, l'impressione è che, rispetto all'uso dell'intelligenza artificiale in medicina, il problema della non discriminazione si ponga soprattutto, più che in relazione all'accesso ai servizi sanitari (come si è invece posta tradizionalmente), in relazione alla qualità delle prestazioni sanitarie erogate²⁹.

28. Cfr. MITTELSTADT 2021, p. 24.

29. Possono certo richiamarsi anche situazioni nelle quali potrebbero manifestarsi disuguaglianze nell'accesso alle nuove tecnologie, come, ad esempio, nel caso in cui i territori o le istituzioni sanitarie *early adopter* godano prima degli altri dei benefici di nuovi interventi farmaceutici o terapeutici realizzati con l'AI: cfr. sul punto MITTELSTADT 2021, p. 4 (anche se questa disuguaglianza, da un lato, non rappresenta una vera e propria discriminazione con riferimento ai profili indicati dal primo comma dell'art. 3 Cost. e, dall'altro, può considerarsi un dato "fisiologico" che riguarda ed ha riguardato in generale tutte le innovazioni in campo medico, anche prima dell'avvento dell'AI); o situazioni in cui un incremento nell'accesso alle cure si associa tuttavia all'erogazione di prestazioni di qualità inferiore: ad esempio, la telemedicina porta le cure in luoghi remoti o con carenza di operatori sanitari, ma di qualità inferiore sotto il profilo della relazione medico-paziente (*ivi*, p. 44).

La qualità della prestazione sanitaria erogata con l'ausilio di sistemi di AI, primi fra tutti i sistemi di apprendimento automatico – o, meglio, la differente qualità delle prestazioni rispetto ai singoli pazienti – dipende in larga misura dalla qualità dei dati utilizzati (e anzitutto di quelli impiegati per addestrare i sistemi automatici): come ha opportunamente osservato l'Organizzazione Mondiale della Sanità, «quando si utilizza l'intelligenza artificiale in ambito sanitario bisogna sempre documentare come e perché dati o set di dati vengono selezionati per addestrare, convalidare e riqualificare il modello»³⁰, in quanto «la qualità dei dati condiziona la sicurezza e l'efficacia dei sistemi di IA» e «consente di evitare distorsioni ed errori»³¹.

I dati di scarsa qualità, che comportano i rischi maggiori per la sicurezza, l'efficacia ma anche per l'equità in senso lato dei sistemi di apprendimento automatico, sono principalmente di due tipi, che vanno tenuti ben distinti: dati distorti o “inquinati” (*biased*) e dati incompleti³².

In particolare, i dati “inquinati” sono quelli che contengono già in sé dei *bias*, delle distorsioni, e, nel nostro caso, quelli che riflettono pregiudizi legati alle categorie tradizionalmente discriminate³³ presenti nelle società occidentali³⁴. Le conseguenze di queste dinamiche sono state indagate ampiamente negli Stati Uniti, caratterizzati dalla presenza di un razzismo sistemico che penalizza i gruppi minoritari³⁵.

Il problema, invece, dei dati incompleti si collega alla scarsa *rappresentatività* dei dati raccolti per

addestrare il sistema. Anche questo aspetto è stato ben evidenziato dall'Organizzazione Mondiale della Sanità, che ha messo in rilievo il rischio che si producano errori quando «i dati utilizzati per produrre il modello non sono pienamente rappresentativi» (*bias* di selezione), oppure quando «il dispositivo di raccolta dei dati fa sì che essi vengano sistematicamente distorti in una direzione particolare» (*bias* di misurazione)³⁶. L'OMS, in particolare, ha inteso sottolineare l'importanza decisiva della completezza dei dati sanitari utilizzati dalle AI mediche³⁷ ricordando che, da un recente studio dell'Università di Stanford, è emerso che il 71% dei dati dei pazienti con cui si addestra la maggior parte degli strumenti diagnostici di intelligenza artificiale utilizzati negli USA proviene da soli tre Stati: California, New York e Massachusetts³⁸.

La scarsa rappresentatività dei dati, tuttavia, non risulta legata soltanto al territorio (e dunque alla scelta delle aree di raccolta delle informazioni), ma anche alle specifiche categorie di persone che i dati rappresentano. Ad esempio, le donne risultano storicamente sotto-rappresentate nelle sperimentazioni cliniche e distorsioni analoghe si registrano anche su base razziale: in particolare, preoccupa in prospettiva lo scarso coinvolgimento delle minoranze etniche o razziali nella ricerca genomica, che rappresenta una lacuna rilevante anche perché gli studi genomici rivestiranno un ruolo decisivo nella personalizzazione delle cure³⁹. Anche il Consiglio d'Europa, infine, ha posto in rilievo il tendenziale sbilanciamento della raccolta

30. WORLD HEALTH ORGANIZATION 2023, p. 10.

31. *Ivi*, p. 27.

32. Sul punto v., per tutti, ZUIDERVEEN BORGESIU 2018, spec. p. 17 ss.

33. Così MITTELSTADT 2021, p. 49.

34. Sul tema sia consentito rinviare a ZUDDAS 2020A.

35. Ad esempio – come riportano MORANA-BALDUZZI-MORGANTI 2022, pp. 146-147 – da un'analisi condotta nel 2022 sulla banca dati di un policlinico universitario di Chicago è emerso che la descrizione dei pazienti lasciava trasparire un diffuso pregiudizio razziale: in particolare, nelle descrizioni dei pazienti afroamericani comparivano molto più frequentemente, rispetto alle descrizioni degli altri pazienti affetti dalle medesime patologie, i termini “hysterical”, “aggressive” e simili (cfr. SUN-OLIWA-PEEK et al. 2022, p. 203 ss.).

36. WORLD HEALTH ORGANIZATION 2023, p. 28.

37. *Ivi*, p. 29.

38. SHANA 2020.

39. Sui temi richiamati si v. l'analisi svolta da MORANA-BALDUZZI-MORGANTI 2022, p. 148 ss. In particolare, i dati sulle donne sono ripresi dal documento del COMITATO NAZIONALE PER LA BIOETICA 2008, mentre in merito alle lacune nella raccolta dei dati sotto il profilo della rappresentatività su base “razziale” in senso lato, le Autrici

dei dati sanitari utilizzati per addestrare i sistemi di apprendimento automatico impiegati in ambito medico a favore dei “maschi bianchi”⁴⁰.

In conclusione, le distorsioni generate dalla scarsa rappresentatività dei dati utilizzati per alimentare i sistemi di AI impiegati in ambito sanitario conducono a prestazioni differenziate in base al territorio e soprattutto alla “categoria” di appartenenza del paziente (dando luogo a vere e proprie discriminazioni nell'erogazione del servizio principalmente in ragione del sesso e della razza); peraltro, a prestazioni migliori – nei termini di diagnosi più affidabili o di terapie più efficaci – per i pazienti appartenenti alle categorie meglio (o più) rappresentate nel *data set* potrebbero simmetricamente corrispondere, nei casi più gravi, veri e propri errori nella diagnosi o nelle scelte terapeutiche per i pazienti meno rappresentati nelle banche dati: in questi casi il ricorso a strumenti di AI per la formulazione di diagnosi o terapie non si limiterebbe a determinare una violazione del principio di non discriminazione, ma produrrebbe un vero proprio danno alla salute dei soggetti discriminati⁴¹.

Un'ulteriore caratteristica dei sistemi di machine learning, che ne impone un utilizzo prudente e ben controllato in particolare in ambito medico, è la loro tendenza a replicare e quindi a cristallizzare le distorsioni, in questo modo amplificandole. Come ha recentemente ribadito il Consiglio d'Europa, senza interventi preventivi adeguati, i pregiudizi sociali saranno “appresi” e “rafforzati” dell'intelligenza artificiale⁴². Soprattutto nei

sistemi di apprendimento automatico, se i dati sono distorti o incompleti – poiché le decisioni “storiche” influenzano le decisioni future – i c.d. “circuiti di feedback” che si producono determinano un ulteriore peggioramento della condizione dei gruppi più svantaggiati⁴³.

Questi fenomeni sono ben noti e sono stati registrati in tutti i settori di utilizzo dell'intelligenza artificiale. Le soluzioni che al momento vengono suggerite per arginare queste derive – e il settore sanitario non fa eccezione: ad esempio, indicazioni in tal senso sono state ribadite anche di recente dal Consiglio d'Europa – sono quelle, per un verso, ovviamente, di migliorare la selezione dei dati utilizzati per alimentare i sistemi di apprendimento automatico, con riguardo sia all'assenza di *bias*, sia all'adeguata rappresentatività del campione considerato; per altro verso, di garantire la sicurezza di tali sistemi attraverso robusti standard di test e validazione che ne precedano l'implementazione⁴⁴.

2.1. Il caso della c.d. medicina potenziativa: disuguaglianza nell'accesso alle prestazioni sanitarie e impatto sulle “condizioni personali” dei cittadini

Un'ultima notazione, relativa al tema dell'eguale accesso alle prestazioni sanitarie che si avvalgono di sistemi di intelligenza artificiale: questo profilo appare particolarmente rilevante in relazione a un peculiare ambito di applicazione delle tecnologie informatiche – il quale, peraltro, forma oggetto di specifica attenzione da parte del codice

segnalano che, ad esempio, da un'indagine condotta sulle banche dati che raccolgono immagini di lesioni della pelle (cfr. ESTEVA–KUPREL–NOVOA et al. 2017, p. 115 ss.) è emerso che la maggior parte dei programmi di machine learning impiegati in campo dermatologico è addestrata con immagini raccolte negli USA, in Australia e in Europa (e dunque riferite essenzialmente a persone *fair skinned*: cfr. ADAMSON–SMITH 2018, p. 1247 ss.).

40. MITTELSTADT 2021, pp. 5 e 49. In particolare, il Consiglio d'Europa, nel ribadire le gravi conseguenze prodotte da tale approccio soprattutto sulle concrete prospettive di cura delle donne, richiama sul punto l'analisi di SAINI 2017: l'Autrice osserva efficacemente come molti modelli clinici trattino le donne alla stregua di “piccoli uomini”, trascurando alcune fondamentali differenze biologiche, come ad esempio la diversa percentuale di grasso corporeo, la maggiore sottigliezza della pelle o il cambiamento dei livelli ormonali durante il ciclo mestruale; fattori che influenzano, talvolta anche sensibilmente, l'efficacia dei farmaci o la risposta immunitaria.

41. Così MORANA–BALDUZZI–MORGANTI 2022, p. 145.

42. Così MITTELSTADT 2021, p. 6.

43. In argomento cfr. per tutti RESTA 2019, p. 199 ss., spec. 214. Inoltre, queste tecnologie non sono accessibili a tutti: questo tuttavia solleva un problema distinto, riguardante l'eguaglianza sostanziale, che esula dall'orizzonte di questo lavoro.

44. Cfr. MITTELSTADT 2021, p. 6.

deontologico – che è quello della c.d. medicina potenziativa.

In particolare, l'art. 76 del codice (*Medicina potenziativa*) qualifica tali interventi come «prestazioni non terapeutiche ma finalizzate al potenziamento delle fisiologiche capacità fisiche e cognitive dell'individuo»: si tratta di prestazioni, come ad esempio gli impianti neuronali, che fanno largo uso di sistemi di intelligenza artificiale⁴⁵. Rispetto all'erogazione di tali prestazioni, il codice di deontologia medica stabilisce numerosi limiti, che vanno dalla tutela della dignità, dell'identità e della integrità della persona, sino al dovere di rifiutare richieste sproporzionate e di alto rischio⁴⁶.

Tuttavia, sebbene tale esigenza non sia espressamente contemplata nel codice, appare di vitale importanza anche garantire un eguale accesso a queste pratiche (che non significa naturalmente stabilire che tutti indistintamente ne abbiano diritto, ma che la distinzione tra aventi diritto e non aventi diritto sia fondata razionalmente su comprovate necessità mediche e non su altri elementi); un'esigenza che va garantita soprattutto al fine di mitigare gli *effetti differenzianti* di tali interventi. La medicina potenziativa, infatti, implica sovente l'utilizzo di tecnologie che *rendono diseguali*; incidendo soprattutto sulle "condizioni personali", che la Costituzione contempla espressamente nel primo comma dell'art. 3 tra gli elementi che, al pari del sesso, della razza o della religione, potrebbero dare origine a trattamenti discriminatori.

Nel caso del ricorso alla medicina potenziativa, il problema della disuguaglianza non si pone soltanto, per così dire, "in entrata", nel senso che vale anche per queste pratiche mediche il divieto di negarne l'accesso per ragioni razziali o di genere; ma si pone anche, per così dire, "in uscita", nel senso che l'accesso o meno a tali pratiche ha un ricaduta

sulle condizioni personali, e principalmente sulle "capacità", come ricorda l'art. 76 del codice, o, più in generale, sulle "abilità" della persona, che risultano potenziate a seguito dell'intervento medico. Con una rilevantissima differenza, peraltro, rispetto a quanto accade a seguito degli interventi medici tradizionalmente incidenti sulle abilità della persona. Finora, infatti, le disuguaglianze nell'accesso ad alcune prestazioni sanitarie (come, ad esempio, gli interventi di chirurgia oculare volti a mitigare la condizione dei soggetti ipovedenti) potevano tradursi in una differenziazione delle condizioni personali (tra che vi accedeva e chi non vi accedeva) che si giocava su quello che potremmo definire il "campo negativo", tra chi riusciva a superare la condizione di disabilità e chi non era messo nella condizione di superarla (o, detto diversamente, si modulava rispetto alla presenza o assenza di disabilità). Con la medicina potenziativa, la partita, per così dire, si gioca (anche) nel "campo positivo" tra chi riesce a potenziare le proprie capacità e chi non è posto nelle condizioni di potenziarle (o, detto diversamente, si modula rispetto alla presenza o assenza di *super-abilità*).

Si tratta, peraltro, di dinamiche nelle quali risultano fortemente coinvolte anche le disuguaglianze di tipo sostanziale, anche in questo caso sia "in entrata" sia "in uscita": "in entrata" perché, considerati i costi ad oggi particolarmente elevati, fino a quando non potrà farsene carico il servizio pubblico, a molte di queste prestazioni potranno concretamente accedere soltanto le fasce di popolazione economicamente più abbienti; "in uscita", perché l'accesso diseguale a tali pratiche appare suscettibile di dar vita a nuove classi sociali di individui "potenziati", dotati di anche di una dignità sociale superiore rispetto agli altri (o, meglio, che potrebbero reclamare il riconoscimento di un valore

45. Sul tema si v., *ex multis*, ZHANG-MA-ZHENG et al. 2020. Per un'analisi delle più ampie ricadute antropologiche delle pratiche mediche in oggetto cfr. WARWICK 2020.

46. La disposizione in esame – nel testo attualmente in vigore a seguito delle modifiche intervenute, come prima ricordato, il 15 dicembre 2017 – stabilisce in particolare che «il medico, sia in attività di ricerca, sia quando gli siano richieste prestazioni non terapeutiche ma finalizzate al potenziamento delle fisiologiche capacità fisiche e cognitive dell'individuo, opera nel rispetto e a salvaguardia della dignità dello stesso in ogni suo riflesso individuale e sociale, dell'identità e dell'integrità della persona e delle sue peculiarità genetiche nonché dei principi di proporzionalità e di precauzione. Il medico acquisisce il consenso informato in forma scritta avendo cura di verificare, in particolare, la comprensione dei rischi del trattamento. Il medico ha il dovere di rifiutare eventuali richieste ritenute sproporzionate e di alto rischio anche a causa della invasività e potenziale irreversibilità del trattamento a fronte di benefici non terapeutici ma potenziativi».

sociale superiore rispetto agli altri consociati); non a caso, l'art. 76 del codice impone al medico di operare «a salvaguardia della *dignità* [dell'individuo] in ogni suo riflesso individuale e *sociale*».

3. Al medica e consenso informato: la libertà di cura in bilico tra necessaria *comprensibilità* dell'informazione richiesta per il consenso e *opacità* dei sistemi di apprendimento automatico

In merito al consenso informato, può essere utile prendere le mosse dalla Carta europea di etica medica, che, pur non richiamando espressamente tale istituto, ne individua con estrema chiarezza il fondamento, stabilendo, nel *Principio* 9, che «la pratica medica implica in ogni circostanza il rispetto costante della vita, dell'autonomia morale e della *libertà di scelta del paziente*». La libertà di scelta, infatti, rappresenta il fondamento del consenso informato anche nel nostro ordinamento costituzionale: in particolare, il consenso informato, «legittimazione e fondamento» di ogni trattamento sanitario⁴⁷, è funzionale all'esercizio del diritto alla salute riguardato come diritto di libertà – a quella, cioè, che viene di norma qualificata come «libertà di cura» – ponendosi come una «proiezione» di tale libertà⁴⁸.

Questo schema trova piena conferma sia nella legislazione ordinaria, sia nella giurisprudenza costituzionale. Nella legislazione ordinaria, si ritrova esattamente questa impostazione nella legge istitutiva del Servizio sanitario nazionale: in particolare, la libertà, intesa come autodeterminazione rispetto alle scelte terapeutiche, è sancita dall'art. 1 della legge 23 dicembre 1978, n. 833, il quale stabilisce che la tutela della salute deve avvenire «nel rispetto della dignità e della libertà della persona umana»; la volontarietà è invece specificata nel successivo art. 33 della legge istitutiva, che sancisce il «carattere di norma volontario» degli accertamenti e dei trattamenti sanitari. Quanto alla giurisprudenza costituzionale, si possono ricordare almeno due pronunce recenti: la sentenza n. 282 del 2002, nella quale si precisa che il medico, nella scelta della pratica terapeutica, «opera le scelte professionali basandosi sullo stato delle conoscenze a disposizione», «sempre con il consenso del paziente»⁴⁹; la sentenza n. 438 del 2008, nella quale il consenso informato viene qualificato come un «vero e proprio diritto della persona»⁵⁰, che dunque si impone non solo agli operatori sanitari ma anche al legislatore⁵¹.

Nel codice deontologico, il consenso informato è espressamente richiesto in relazione a numerose attività svolte dal medico⁵², ma le norme

47. Così Cass. civ., I sez., sentenza n. 21748 del 16 ottobre 2007 (sul c.d. «caso Englaro»), punto 6 parte motiva; la Suprema Corte, peraltro, aveva già affermato a partire dal 2001 che la manifestazione del consenso del paziente costituisce un presupposto di liceità del trattamento medico chirurgico (cfr. in argomento MORANA 2021, pp. 145 e 157 ss.).

48. Così, da ultimo, MORANA-BALDUZZI-MORGANTI 2022, p. 145. Il consenso informato, dunque, trova un fondamento costituzionale – come la stessa libertà di cura – nel secondo comma dell'art. 32 Cost., in forza del quale «nessuno può essere obbligato a un determinato trattamento sanitario se non per disposizione di legge». La regola, pertanto, è la libertà di rifiutare i trattamenti sanitari, e dunque la volontarietà dei trattamenti: ma, poiché è volontario solo quel trattamento sanitario per il quale sia stato acquisito il consenso, la consensualità è «un corollario necessario» della volontarietà (così MORANA 2021, p. 165).

49. Cfr. punto 4 considerato in diritto.

50. *Ibidem*.

51. Cfr. sul punto MORANA 2021, p. 163.

52. In particolare, il consenso è specificamente richiesto per: il trattamento dei dati personali e la costituzione, gestione e utilizzo di banche dati degli assistiti (art. 11); il trattamento di dati sensibili idonei a rivelare lo stato di salute (art. 12); la prescrizione di farmaci non registrati o non autorizzati al commercio (art. 13); la gestione del rischio clinico (art. 14); l'adozione di sistemi e metodi di prevenzione, diagnosi e cura non convenzionali (art. 15); l'arruolamento in protocolli di ricerca (art. 25); la trasmissione ad altro collega delle informazioni utili alla continuità delle cure a seguito della risoluzione della relazione di cura (art. 28); il prelievo da vivente (art. 41); gli interventi sul genoma umano (art. 45); la prescrizione o l'esecuzione di indagini

fondamentali dedicate all'istituto in esame sono contenute nel Titolo V, segnatamente agli articoli 33 e 35. In particolare, l'art. 35 disciplina il consenso, mentre l'art. 33 disciplina i caratteri dell'informazione e della comunicazione con la persona assistita.

La collocazione topografica delle due disposizioni, da un lato, riflette la priorità logica e cronologica dell'informazione rispetto al consenso "informato"; dall'altro, fa emergere una separazione tra due situazioni di vantaggio – il diritto ad esprimere il consenso o il dissenso rispetto ai trattamenti sanitari ed il diritto a ricevere informazioni sui trattamenti sanitari – che rappresentano due diritti distinti sotto il profilo costituzionale⁵³. L'impostazione codicistica, che mira a disciplinare specificamente i caratteri del consenso e i

caratteri dell'informazione, rappresenta peraltro una "costante": essa, infatti, da un lato, riproduce l'impianto presente nella Convenzione di Oviedo del 1997 e, dall'altro, è stata ripresa dalla legge italiana sul consenso informato del 2017⁵⁴.

Relativamente ai caratteri del consenso, l'art. 35 del codice precisa anzitutto che la competenza ad acquisirlo spetta esclusivamente al medico (il che, come vedremo, porrà un problema nella prospettiva di una interlocuzione diretta uomo-macchina); precisa inoltre che il consenso deve precedere la diagnosi o la terapia (il secondo comma stabilisce in particolare che «il medico non intraprende né prosegue in procedure diagnostiche e/o interventi terapeutici senza la preliminare acquisizione del consenso informato o in presenza di dissenso informato»)⁵⁵ e ne prescrive la formulazione in

predittive (art. 46); la sperimentazione umana (art. 48); le attività diagnostico-terapeutiche con finalità estetiche (art. 76-*bis*).

53. Nella prospettiva costituzionale, infatti, il diritto del paziente ad essere informato sulle cure e sul proprio stato di salute non è solo strumentale al godimento della libertà di cura – non è cioè soltanto servente rispetto alla formazione consapevole del consenso, in base allo schema per cui solo un'adeguata informazione determina quella consapevolezza necessaria affinché il consenso sia validamente prestato e risulti come tale piena espressione della libertà di cura – ma è anche un diritto autonomo rispetto a tale libertà (cfr. in argomento MORANA 2021, p. 169). L'istituto del consenso informato, pertanto, coinvolge – come si accennava – due diritti diversi, entrambi espressione di specifici profili del diritto alla salute: il diritto alla salute come diritto di libertà, qualificabile come libertà di cura, cioè come diritto di acconsentire alle cure o di rifiutarle (che ha come corollario la volontarietà dei trattamenti sanitari); e il diritto alla salute come diritto a ricevere informazioni sui trattamenti sanitari, come diritto cioè ad essere informato sulle cure e sul proprio stato di salute. Quest'ultima facoltà può essere esercitata al fine di acconsentire o meno ai trattamenti sanitari, ma non solo: le persone sottoposte a trattamenti sanitari obbligatori perdono il primo diritto ma non il secondo, in quanto la perdita della consensualità non comporta la perdita del diritto a ricevere informazioni sul trattamento. Tale diritto discende direttamente dal necessario «rispetto della persona umana» che il secondo comma dell'art. 32 Cost. impone come limite espressamente rivolto ai trattamenti sanitari obbligatori (seppure dotato, come vedremo, di una valenza generale): una forma di elementare rispetto della dignità umana, infatti, impone che l'obbligato al trattamento sanitario non sia costretto a riceverlo «in uno stato di cecità informativa» (*ivi*, 170).

54. Legge 22 dicembre 2017, n. 219, *Norme in materia di consenso informato e di dichiarazioni anticipate di trattamento*.

55. La Convenzione di Oviedo già stabiliva, all'art. 5, primo comma, che un intervento in campo sanitario potesse essere effettuato solo dopo che l'interessato avesse prestato il suo consenso "libero e informato" (aggettivazione a sua volta ripresa dalla Carta dei diritti fondamentali dell'Unione europea, all'art. 3), precisando il carattere preventivo anche delle informazioni (cfr. art. 5, secondo comma). La "libertà" del consenso è stata recentemente ribadita dal Consiglio d'Europa, che ha sottolineato come la norma in esame renda chiara l'autonomia del paziente rispetto all'operatore sanitario e impedisca l'affermarsi di approcci paternalistici che potrebbero condurre ad ignorare i desideri del paziente (cfr. MITTELSTADT 2021, p. 23). Ripropone la medesima formulazione dell'art. 35 del codice la legge n. 219/2017, all'art. 1, primo comma (che configura il consenso informato come una condizione in assenza della quale «nessun trattamento sanitario può essere iniziato o proseguito», ad esclusione dei casi espressamente previsti dalla legge).

forma scritta e sottoscritta o equivalente⁵⁶. Il carattere necessariamente “informato” del consenso, infine, è deducibile (anche) dalla rubrica dell’art. 35 del codice, che parla di *Consenso e dissenso informato*.

Relativamente ai caratteri che le informazioni offerte devono possedere (anche) affinché il consenso possa dirsi informato e dunque risulti validamente espresso, due sono essenzialmente gli elementi che rivestono un’assoluta centralità sia nel codice deontologico, sia nei diversi atti normativi che affrontano questa tematica, sia antecedenti che successivi: la *completezza* e la *comprensibilità*⁵⁷. Un ulteriore dato rilevante è che questi due caratteri fondamentali dell’informazione che va offerta al paziente si condizionano reciprocamente, collocandosi in una sorta di rapporto di *trade-off*.

In ordine alla *completezza*, questo requisito è ribadito sia dalla legge n. 219/2017 (che aggiunge anche la necessità che le informazioni siano *aggiornate*)⁵⁸, sia dalla Corte di Cassazione⁵⁹, mentre la Convenzione di Oviedo richiede informazioni

“adeguate”: un concetto che appare più ampio – in quanto esteso anche alle capacità del paziente di comprenderle – evocato anch’esso dalla Corte di Cassazione⁶⁰ e ribadito dalla Corte costituzionale nella sentenza n. 438 del 2008, che riafferma la necessità di offrire informazioni adeguate al fine di garantire al paziente la “libera e consapevole scelta” e, quindi, «la sua stessa libertà personale, conformemente all’art. 32, secondo comma, della Costituzione»⁶¹.

L’oggetto dell’informazione – la cui estensione va indagata per comprendere in che termini possa considerarsi “esaustiva” – risulta estremamente ampio. In particolare, il codice deontologico individua due grandi ambiti: le condizioni di salute (richiamate anche dalla legge n. 219/2017, che ribadisce, all’art. 1, il diritto di ogni persona di conoscere le proprie condizioni di salute) e l’intervento diagnostico-terapeutico. Segnatamente, in relazione al secondo ambito, si identificano una serie di elementi specifici, che vanno dal percorso diagnostico, alla prognosi, alla terapia, alle alternative, ai

56. La legge n. 219/2017 stabilisce più dettagliatamente che «il consenso informato, acquisito nei modi e con gli strumenti più consoni alle condizioni del paziente, è documentato in forma scritta o attraverso videoregistrazioni o, per la persona con disabilità, attraverso dispositivi che le consentano di comunicare» (art. 1, comma 4), mentre la Carta dei diritti fondamentali dell’Unione europea rinvia sul punto alle «modalità definite dalla legge» (art. 3). Sia la Convenzione di Oviedo sia la legge sul consenso informato precisano inoltre che il consenso è revocabile: cfr. l’art. 5, terzo comma, della Convenzione – il quale stabilisce che l’interessato «può revocare liberamente il consenso in ogni momento» – e l’art. 1, comma 5, della legge sul consenso informato, che consente la revoca in qualsiasi momento, anche quando questa comporti l’interruzione del trattamento sanitario. Il diritto di revocare il consenso, peraltro, è desumibile in via diretta dall’art. 32 Cost., secondo comma (in quanto espressione della libertà di cura), così come il diritto di rifiutare trattamenti sanitari anche se da essi dipende la sopravvivenza dell’interessato (anche sul punto cfr. l’art. 1, comma 5, della legge sul consenso informato). In argomento cfr. anche la succitata sentenza della Corte di Cassazione n. 21748 del 2007, in cui si ribadisce il diritto del paziente a non prestare il proprio consenso anche quando il trattamento sanitario sia indispensabile per il suo mantenimento in vita, affermando con nettezza la radice costituzionale sia del diritto del paziente a rifiutare le cure, sia del correlato «dovere del medico di astenersi da ogni attività diagnostica o terapeutica se manchi il consenso del paziente, anche se tale astensione possa provocare la morte» (cfr. punto 6.1 parte motiva); si v. inoltre la più recente sentenza Cass. civ., III sez., n. 29469 del 2020, nella quale si afferma il diritto di rifiutare trattamenti sanitari per motivi religiosi (in quel caso si trattava di un’emotrasfusione a beneficio di un Testimone di Geova). Nel nostro ordinamento, in sostanza, non esiste il dovere di curarsi (a patto, tuttavia, che l’espressione della volontà di rifiutare le cure sia informata, autentica e attuale).

57. In particolare, l’art. 33 del codice deontologico stabilisce che l’informazione deve essere “comprensibile” ed “esaustiva”.

58. Cfr. art. 1, comma 3.

59. Cfr. ad esempio Cass. civ., III sez., n. 5444 del 14 marzo 2006 (su cui anche *infra*, nt. 62).

60. V. *infra*, nt. 65.

61. Punto 4 considerato in diritto.

rischi⁶². Con specifico riferimento a questi ultimi, vale ricordare quanto precisato sul punto dalla Corte di Cassazione, che ha individuato un preciso limite all'ampiezza di contenuto dell'obbligo informativo, circoscrivendo tale obbligo ai soli rischi *prevedibili* (come peraltro correttamente previsto dallo stesso codice deontologico), al fine di «contemperare l'esigenza di informazione con la necessità di evitare che il paziente, per una qualsiasi remotissima eventualità, eviti di sottoporsi anche ad un banale intervento»⁶³: anche la questione della prevedibilità dei rischi, come vedremo, si pone in modo peculiare rispetto ai trattamenti sanitari operati con l'ausilio di sistemi di AI, in quanto prevedere i rischi connessi all'uso di tali sistemi risulta ad oggi particolarmente difficile, sia per l'assenza di riscontri sugli effetti a medio e lungo termine e nell'uso di massa di tecnologie spesso agli esordi, sia per le oggettive difficoltà di prevedere l'output dei software dotati di maggiore autonomia.

La *comprensibilità* delle informazioni fornite è parimenti ribadita dalla legge n. 219/2017, che richiede – all'art. 1, terzo comma – che la persona sia informata in modo, tra l'altro, «a lei comprensibile». Il concetto è poi riaffermato dal codice deontologico in relazione alle modalità di comunicazione: il secondo comma dell'articolo 33 stabilisce infatti che il medico «adeguа la comunicazione alla capacità di comprensione» della persona assistita o del suo rappresentante legale. Impostazione

che si ritrova anche nella relazione esplicativa della Convenzione di Oviedo, in cui si precisa che le informazioni devono essere fornite ai pazienti «in modo facilmente comprensibile»⁶⁴; ed è ribadita dalla Corte di Cassazione, la quale ha precisato che le spiegazioni fornite dal medico devono essere dettagliate e «adeguate al livello culturale» del paziente (e che dunque, a tal fine, non è sufficiente la sola apposizione della firma nel modulo prestampato)⁶⁵.

Per quanto riguarda, infine, il potenziale *trade off* tra adeguatezza e completezza, la Corte di Cassazione ha correttamente evidenziato come l'adeguatezza (che impone di fornire informazioni adeguate al livello culturale del paziente) non debba andare a detrimento della completezza: la «qualità del paziente» è infatti «irrilevante» al fine di «stabilire se vi sia stato o meno consenso informato, potendo essa incidere solo sulle modalità di informazione, in quanto l'informazione deve sostanziarsi in spiegazioni dettagliate ed adeguate al livello culturale del paziente, con l'adozione di un linguaggio che tenga conto del suo particolare stato soggettivo e del grado delle conoscenze specifiche di cui dispone»⁶⁶; ciò vale ad escludere che la qualità del paziente possa invece incidere sul *contenuto* dell'informazione⁶⁷.

Problema, quest'ultimo, che rischia di aggravarsi ulteriormente a seguito dell'utilizzo dei sistemi di AI in medicina, stante la necessità di fornire

62. L'art. 33 del codice deontologico prescrive che l'informazione debba riguardare: la prevenzione, il percorso diagnostico, la diagnosi, la prognosi, la terapia, le eventuali alternative diagnostico-terapeutiche, i prevedibili rischi e complicanze, i comportamenti che il paziente dovrà osservare nel percorso di cura. La Convenzione di Oviedo richiede, più sinteticamente, vengano fornite informazioni «sullo scopo e sulla natura dell'intervento, nonché sulle sue conseguenze e rischi» (art. 5, secondo comma). La legge n. 219/2017 afferma il diritto di ogni persona di conoscere le proprie condizioni di salute e di ricevere informazioni riguardo a: la diagnosi, la prognosi, i benefici ed i rischi degli accertamenti diagnostici e dei trattamenti sanitari, le possibili alternative, le conseguenze dell'eventuale rifiuto del trattamento sanitario e dell'accertamento diagnostico o della rinuncia ai medesimi, incluso il rifiuto di ricevere informazioni e la possibilità di incaricare altri di riceverle (art. 1, comma 3). La Corte di Cassazione, infine, ha affermato sin dal 2006 che l'informazione fornita al paziente deve metterlo «in condizione di assentire al trattamento sanitario con una volontà consapevole delle sue implicazioni» (così Cass. civ., III sez., n. 5444 del 14 marzo 2006, punto 3.1 parte motiva).

63. Cass. civ., III sez., sentenza n. 364 del 15 gennaio 1997 (la pronuncia è ricordata anche da MORANA-BALDUZZI-MORGANTI 2022, p. 137).

64. Cfr. sul punto MITTELSTADT 2021, p. 45.

65. Cfr. Cass. civ., III sez., sentenza n. 19220 del 20 agosto 2013, punto 2.9 parte motiva.

66. *Ibidem*. In tema cfr. ampiamente MORANA 2021, pp. 157 ss.

67. Così MORANA-BALDUZZI-MORGANTI 2022, p. 136.

informazioni complete concernenti anche il funzionamento di sistemi informatici estremamente complessi e di conseguenza scarsamente comprensibili anche per i pazienti di medio livello culturale.

3.1. I rischi di “corto circuito” legati all’obbligo di illustrare al paziente le logiche di funzionamento dell’intelligenza artificiale

Per quanto riguarda gli interventi medici che prevedono l’utilizzo di tecnologie informatiche, vanno richiamate anzitutto le norme del codice deontologico che stabiliscono l’obbligo di acquisire il consenso informato in ambiti in cui possono essere coinvolti software di intelligenza artificiale: tra queste, l’art. 14, che lo richiede per la gestione del rischio clinico (si considerino in proposito i rischi specifici legati all’uso di AI) e l’art. 46, che lo richiede per effettuare indagini predittive (ambito nel quale si registra un ricorso crescente a sistemi di intelligenza artificiale).

Al di là delle specifiche situazioni disciplinate dalle disposizioni evocate, il codice prevede all’art. 78 una norma di carattere generale, che impegna espressamente il medico a garantire, «nell’uso degli strumenti informatici» (dunque, si ritiene, ogni qualvolta egli faccia uso di tali strumenti) «l’acquisizione del consenso»; consenso che, in base a quanto osservato⁶⁸, non può dirsi valido se non è “informato”. La disposizione, peraltro, prosegue incaricando il medico – a ulteriore conferma della necessità di offrire al paziente un’adeguata informazione – di garantire, «nell’uso di tecnologie di informazione e comunicazione di dati clinici», la «consapevole partecipazione» della persona assistita⁶⁹.

In ordine ai caratteri dell’informazione necessaria al consenso, se – come abbiamo visto – in linea generale rivestono un ruolo centrale i requisiti della completezza e della comprensibilità (ed esiste, entro certi limiti, una relazione inversa tra questi

due elementi), tale centralità (e il relativo *trade off*) si ripropone in termini rafforzati nel caso di interventi diagnostico-terapeutici effettuati con l’ausilio di sistemi di intelligenza artificiale.

Segnatamente, in queste specifiche circostanze: la completezza delle informazioni implica che si debba riferire al paziente anzitutto se, o il fatto che vengano utilizzati sistemi di AI nell’attività diagnostico-terapeutica; la comprensibilità dell’informazione implica che si debba anche spiegare *quanto e come* i sistemi di AI incidano sulla diagnosi o sulla terapia.

La necessità di riferire al paziente del ricorso a sistemi di intelligenza artificiale nello svolgimento dell’attività medica può dedursi anzitutto dal *Principio 13* della Carta europea di etica medica, in base al quale «il medico deve informare il paziente se le condizioni morali e tecniche sono tali da impedirgli di agire in piena autonomia». Certo, l’utilizzo di sistemi di AI va letto più nella prospettiva dell’ausilio che in quella dell’impedimento; tuttavia, una volta che il medico decida di avvalersi di tali tecnologie, affidandosi anche solo in parte alla macchina per compiere la propria attività diagnostica o terapeutica, è evidente che, se tale affidamento a strumenti tecnici dotati di margini di scelta autonoma si traduce in una limitazione alla “piena autonomia” nello svolgimento dei suoi compiti, il medico è tenuto ad informarne il paziente (anche se non si richiede espressamente il consenso).

L’obbligo, a carico dell’operatore sanitario, di informare il paziente dell’utilizzo di intelligenza artificiale nel procedimento che ha portato alla diagnosi o alla proposta terapeutica è stato invece sancito espressamente⁷⁰ sia dal Comitato Nazionale per la Bioetica, sia dal Comitato Nazionale per la Biosicurezza, le Biotecnologie e le Scienze della Vita⁷¹ (e, in parte, dallo stesso Consiglio di superiore di sanità)⁷².

68. Cfr. *supra*, nt. 53.

69. In particolare, sulla “partecipazione” del paziente all’intervento medico cfr. GRASSO 2011, p. 49, che concepisce il consenso informato come «procedimento partecipato» che «cerca di mantenere insieme, in una posizione diversa, ma di pari dignità, paziente e medico».

70. Come ricordato, da ultimo, da MORANA–BALDUZZI–MORGANTI 2022, p. 139.

71. Cfr. COMITATO NAZIONALE PER LA BIOETICA E COMITATO NAZIONALE PER LA BIOSICUREZZA, LE BIOTECNOLOGIE E LE SCIENZE DELLA VITA 2020, p. 14.

72. Cfr. CONSIGLIO SUPERIORE DI SANITÀ 2021, p. 30 ss.

Il vero problema, tuttavia, non riguarda il *se*, ma il *come*, cioè la necessità di informare il paziente sulle logiche di funzionamento del sistema di AI impiegato (o, per utilizzare la formula contemplata dal Regolamento europeo sulla protezione dei dati, la “logica utilizzata”) per il trattamento informatizzato dei dati sanitari⁷³.

Queste logiche, infatti, presentano amplissimi margini di opacità. Un’opacità che, come è noto, ha molte facce. Le ragioni che la giustificano, infatti, non sono soltanto di natura “soggettiva”: non derivano cioè solo dalle limitate cognizioni tecniche del medico o del paziente (e, segnatamente, dalla capacità del medico di spiegare il funzionamento di complessi sistemi informatici e dalla capacità del paziente di comprenderlo). Ma esistono anche ragioni in certo senso “oggettive”: da un lato, occorre fare i conti con l’opacità di origine “commerciale”, derivante dalla scelta dei produttori di sistemi di AI di non rivelare aspetti essenziali del funzionamento degli algoritmi in quanto coperti dal segreto industriale; dall’altro, sussiste anche un’opacità “intrinseca”, tipica dei sistemi di machine learning, che riescono a processare enormi volumi di dati attraverso tecniche elaborative complesse, seguendo percorsi che risultano, per certi versi, ignoti agli stessi programmatori, in quanto

le correlazioni individuate dalla macchina hanno un’origine statistica, non – necessariamente – causale⁷⁴. Questa difficoltà, peraltro, è stata segnalata, con specifico riferimento alle intelligenze artificiali utilizzate in ambito medico, dall’Organizzazione Mondiale della Sanità, che ha osservato come non vi sia «piena comprensione di come tali sistemi di AI possano funzionare»⁷⁵.

Ciò premesso (e considerata la presenza di limiti “oggettivi” comunque non valicabili), concentriamoci sui limiti “soggettivi”.

Anzitutto, le difficoltà che può incontrare il medico nella spiegazione di sistemi informatici complessi è aggravata dalla mole e dalla varietà di informazioni specifiche richieste ai fini del consenso informato qualora si ricorra all’impiego dell’intelligenza artificiale. In base a quanto sostenuto, ad esempio, dal Consiglio d’Europa⁷⁶, andrebbe spiegato al paziente (ma, preliminarmente, anzitutto al medico): a) come funziona il sistema di intelligenza artificiale (in termini generali); b) come è stato prodotto l’output specifico (ad esempio, quando un sistema di AI interpreta immagini o elabora diagnosi, dovrebbe essere il sistema stesso a spiegare il proprio processo decisionale)⁷⁷; c) come è stato progettato e testato il sistema di AI⁷⁸; d) come il sistema è “governato” (cioè, quali sono le regole e

73. In particolare, l’art. 15 (rubricato *Diritto di accesso dell’interessato*) del Regolamento UE 2016/679 (GDPR) stabilisce che «l’interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l’accesso ai dati personali e alle seguenti informazioni: [...] h) l’esistenza di un processo decisionale automatizzato e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l’importanza e le conseguenze previste di tale trattamento per l’interessato».

74. Si tratta dell’arcinota *black box*, secondo la fortunata formula proposta da Frank Pasquale: sul tema cfr. ZUDDAS 2020.

75. WORLD HEALTH ORGANIZATION 2023, *Foreword*, p. V.

76. MITTELSTADT 2021, p. 5.

77. *Ivi*, pp. 5 e 46. In proposito, vale ricordare che la Corte di Cassazione ha recentemente sostenuto (Cass. Civ., Sez. I, ordinanza n. 30123 del 10 ottobre 2023) – confermando nella sostanza l’orientamento espresso dal Consiglio di Stato – che, al fine di integrare i presupposti di un consenso “libero e specifico” (il quale, come l’output, riguarda il funzionamento del sistema in una “specifica” circostanza), chi intenda prestarlo deve conoscere tutte le informazioni riguardanti il processo di formazione del risultato della macchina; per cui, se l’interessato conosce solo l’output e non l’iter logico ad esso sotteso, il consenso non potrà dirsi validamente prestato (cfr. in proposito DI MARTINO 2024).

78. Anche l’Organizzazione Mondiale della Sanità richiede, per le intelligenze artificiali utilizzate in ambito sanitario, una «documentazione accurata e completa» che consenta di «preindicare e documentare processi, metodi, risorse e decisioni prese nella progettazione iniziale [del prodotto, fino alla] post-implementazione», illustrando l’intero “ciclo di vita” dell’intelligenza artificiale: così WORLD HEALTH ORGANIZATION 2023, p. 8.

i protocolli che governano il suo utilizzo); e) quali informazioni sono necessarie per studiarne il funzionamento.

In particolare, secondo il Consiglio d'Europa, i primi due gruppi di informazioni – sulla funzionalità “interna” e sul comportamento “esterno” – garantirebbero la “interpretabilità” del sistema di AI, mentre gli altri due insiemi di informazioni – sulla progettazione e sul governo del sistema – ne garantirebbero la “trasparenza”⁷⁹.

Risulta a questo punto con assoluta evidenza come, nel caso di ricorso a sistemi di AI in ausilio all'intervento medico, appaia particolarmente marcato il *trade off* tra *completezza* delle informazioni e *comprensibilità complessiva* dell'insieme di aspetti e di dettagli che andrebbero comunicati e spiegati⁸⁰.

In particolare, l'esigenza ineludibile che le informazioni siano comprensibili impone di considerare con grande attenzione non soltanto la capacità del medico di spiegare il funzionamento di sistemi informatici complessi, ma – anche e soprattutto – la capacità dei pazienti di accogliere tali spiegazioni. Sul punto il Consiglio d'Europa si è espresso molto nettamente affermando che spesso i pazienti non hanno un livello di consapevolezza sufficiente per comprendere le logiche di funzionamento dell'intelligenza artificiale⁸¹.

Alla difficoltà del paziente “medio” nel comprendere il funzionamento di tali sistemi si associa inoltre il timore che i soggetti più fragili culturalmente o più refrattari alle nuove tecnologie (come, ad esempio, i pazienti più anziani) oppongano un rifiuto preconcepito al loro impiego. Anche in questi casi, comunque, permane l'obbligo del medico

di illustrare i rischi prevedibili (anche se di natura straordinaria) legati agli interventi diagnostici o terapeutici operati con l'ausilio di sistemi di AI, pena l'affermarsi di derive paternalistiche⁸².

Vanno poi considerate alcune situazioni particolarmente complicate: ad esempio, nel caso in cui debba effettuarsi un intervento chirurgico assistito da un robot, il paziente andrebbe informato – in modo completo e comprensibile – sia dei rischi dell'operazione, sia del grado di autonomia della macchina e delle possibilità di intervento del chirurgo (e la revoca del consenso informato deve poter avvenire in ogni momento, sia prima dell'inizio dell'operazione sia durante la terapia)⁸³.

Non vanno infine trascurate alcune ricadute pratiche delle questioni affrontate: non solo, infatti, in linea generale, gli algoritmi sono difficili da spiegare (e sul punto il Consiglio d'Europa ha ribadito molto chiaramente che la difficoltà di spiegare il funzionamento dell'IA è una “sfida fondamentale” per il consenso informato)⁸⁴; ma, nel caso specifico di intelligenze artificiali utilizzate in campo medico, è estremamente complicato inserire informazioni tecniche dettagliate sul funzionamento di sistemi informatici complessi in un modulo per il consenso informato⁸⁵.

Dobbiamo allora rassegnarci ad ambire soltanto – come è stato efficacemente osservato⁸⁶ – ad un «consenso consapevolmente disinformato»?

In realtà, sono attualmente allo studio del Consiglio d'Europa alcune proposte di integrazione della Convenzione di Oviedo, volte ad introdurre nel testo: da un lato, un insieme di nuovi standard della pratica medica tesi a definire sia *quali* informazioni andrebbero fornite in merito ai sistemi di

79. Così MITTELSTADT 2021, pp. 47-48.

80. Senza contare che il medico, pur non essendo tenuto «a svolgere per ogni cliente una lezione di scienza medica» (per usare le parole di CATTANEO 1957, p. 962), sembrerebbe quasi obbligato, paradossalmente, a svolgere una lezione di scienza informatica...

81. MITTELSTADT 2021, pp. 5 e 46.

82. In argomento si v. in particolare le riflessioni contenute in MORANA-BALDUZZI-MORGANTI 2022, pp. 140-141.

83. Cfr. sul punto BIANCARDO 2021, p. 144.

84. MITTELSTADT 2021, p. 5. Sui progressi raggiunti nel campo della c.d. *explainability* dei sistemi di AI utilizzati a fini diagnostici si v., per tutti, FELDMAN-KUCK-HEMMERLING 2012, p. 1777 ss.

85. Così MORANA-BALDUZZI-MORGANTI 2022, p. 150. Con la possibile conseguenza di “raffreddare” ulteriormente il rapporto di fiducia medico-paziente, già potenzialmente irrigidito dall'uso sistematico della forma scritta (cfr. in proposito BALDUZZI-PARIS 2008, p. 4959).

86. CASONATO 2019, p. 101 ss.

AI utilizzati per diagnosi e trattamenti, sia *come* tali informazioni dovrebbero essere comunicate al paziente⁸⁷; dall'altro, l'istituzione di un registro pubblico dei sistemi di intelligenza artificiale medica in uso, contenente una descrizione standardizzata di ciascun sistema, con l'indicazione, tra l'altro, dello scopo del sistema, dei metodi di funzionamento (deep learning, regressione, ecc.) e dei test a cui è stato sottoposto (con riguardo, ad esempio, all'accuratezza o al rispetto del principio di non discriminazione)⁸⁸.

3.2. Tra consenso informato e relazione di cura: il ruolo dell'informazione (e dell'empatia) nella costruzione del rapporto fiduciario tra medico e assistito

Offrire al paziente un quadro il più possibile completo e – insieme – comprensibile (pur con i limiti che abbiamo visto) sull'uso di strumenti di AI in medicina – ed ottenere in base a queste informazioni un consenso consapevole del paziente – è importante anche per preservare la relazione di cura tra medico e assistito.

Il consenso informato, infatti, non è solo un diritto del paziente⁸⁹, ma è anche la base del rapporto medico-paziente⁹⁰. Così è stabilito espressamente dalla legge n. 219/2017, che all'art. 1, secondo comma, qualifica il consenso informato come fondamento della «relazione di cura e di fiducia tra paziente e medico» e punto di

incontro tra «l'autonomia decisionale del paziente e la competenza, l'autonomia professionale e la responsabilità del medico»; e così è ribadito, con specifico riferimento all'AI in medicina, dal Consiglio d'Europa, che – muovendo dai valori sui quali la Convenzione di Oviedo imposta la relazione medico-paziente (espressione, a loro volta, dei diritti umani riguardanti la salute che ne hanno ispirato la formulazione), tra i quali compare espressamente (insieme alla dignità umana, l'integrità fisica, il primato degli interessi del paziente rispetto agli interessi sociali e scientifici, la non discriminazione) il consenso informato – ha definito il consenso informato e la trasparenza “valori chiave” nella relazione medico-paziente mediata dall'intelligenza artificiale⁹¹. La consensualità (che non è solo la regola generale per i trattamenti sanitari, ma è espressamente prevista dall'art. 78 del codice deontologico rispetto all'uso delle tecnologie informatiche) esige infatti che la strutturale “asimmetria informativa” che caratterizza la relazione medico-paziente sia superata o comunque ridotta al minimo attraverso un flusso informativo chiamato a svilupparsi al suo interno⁹². Tutto ciò comporta il superamento della concezione paternalistica e unidirezionale della relazione in esame: la salute, in particolare, va “costruita” nell'ambito di una vera “alleanza terapeutica” tra medico e paziente – “corollario immediato” della libertà di cura⁹³ – considerando quest'ultimo come soggetto attivo che concorre, pur con un ruolo diverso, al

87. Cfr. MITTELSTADT 2021, p. 57.

88. *Ivi*, p. 60. In ordine al necessario rispetto del principio di non discriminazione, il Consiglio d'Europa ha sottolineato come, a tal fine, occorra realizzare una più ampia raccolta di dati sensibili sui gruppi protetti per effettuare i test sui bias (*ivi*, p. 61).

89. Come ha sancito espressamente la Corte di cassazione: cfr. sentenza n. 21748 del 2007, in cui si afferma che il principio del consenso informato «esprime una scelta di valore nel modo di concepire il rapporto tra medico e paziente, nel senso che detto rapporto appare fondato prima sui diritti del paziente e sulla sua libertà di autodeterminazione terapeutica che sui doveri del medico» (cfr. punto 6 parte motiva).

90. In argomento v., per tutti, MORANA 2021, p. 145.

91. Cfr. MITTELSTADT 2021, p. 5.

92. Così MORANA 2021, p. 166 (flusso informativo che, sottolinea l'A., rappresenta un «momento essenziale del rapporto di cura»). In termini analoghi, da ultimo, MORANA-BALDUZZI-MORGANTI 2022, p. 132, in cui si ribadisce che, affinché il consenso sia consapevole, è indispensabile che «venga superato, o quantomeno ridotto nella misura maggiore possibile», il «disequilibrio nel possesso di informazioni che *ex ante* contraddistingue la relazione tra il medico e il paziente». Sulla sostanziale impossibilità di superare l'asimmetria informativa tra medico e paziente si v. le considerazioni di GRASSO 2011, spec. pp. 6 e 47 ss.

93. Così MORANA-BALDUZZI-MORGANTI 2022, p. 131.

perseguimento delle finalità costituzionali sancite dall'art. 32 Cost.⁹⁴

In questa prospettiva, quando l'intervento diagnostico-terapeutico si realizzi attraverso il ricorso a sistemi di AI, il medico, principale "punto di assistenza" per il paziente, può operare come mediatore tra l'intelligenza artificiale e il paziente: il medico, cioè, quale primo destinatario degli output provenienti dal sistema, agirebbe come "traduttore" per il paziente (sempre che, ovviamente – come ricordato *supra*, par. 3.1 – il sistema sia in grado di segnalare al medico le ragioni che giustificano quell'output); se, invece, si realizzasse un rapporto diretto tra intelligenza artificiale e paziente, il sistema informatico dovrebbe essere in grado spiegare all'assistito il proprio processo decisionale⁹⁵.

Il problema, però, è che il codice deontologico richiama un tema centrale nel rapporto medico-paziente, che è quello dell'empatia: l'art. 33 del codice, infatti, nel disciplinare (al secondo comma) le modalità di comunicazione delle informazioni al paziente, non sottolinea soltanto la necessità che l'informazione sia comprensibile⁹⁶, ma aggiunge che la comunicazione deve «tene[re] conto della sensibilità e reattività emotiva» dei medesimi, «in particolare in caso di prognosi gravi o infauste, senza escludere elementi di speranza». Tutto ciò, come può facilmente immaginarsi, rappresenta un grave problema nell'ipotesi in cui sia la macchina a gestire direttamente il dialogo col paziente⁹⁷.

4. Al medica e relazione di cura: la progressiva trasformazione del rapporto medico-paziente in rapporto medico-paziente-intelligenza artificiale

Il codice di deontologia medica dedica il Titolo III ai *Rapporti con la persona assistita* e specificamente l'art. 20 alla *Relazione di cura*⁹⁸.

In particolare, il primo comma dell'art. 20 marca la distinzione di ruoli tra medico e paziente sottolineando la reciproca autonomia: la norma stabilisce infatti che «la relazione tra medico e paziente è costituita sulla libertà di scelta e sull'individuazione e condivisione delle rispettive autonomie e responsabilità». Il fondamento costitutivo della relazione di cura viene quindi individuato anzitutto nella "libertà di scelta": questo vale a rafforzare ulteriormente, anche muovendo da questa prospettiva, il nesso tra la relazione di cura e il consenso informato, che trova egualmente – come abbiamo visto – fondamento nel diritto alla salute come diritto di libertà.

La relazione tra medico e paziente assume invece, nel comma successivo, un tono differente: se il primo comma li distingue, il secondo li avvicina, indicando come obiettivo da raggiungere l'*alleanza* tra i due soggetti: «il medico – prosegue infatti l'art. 20 – nella relazione persegue l'alleanza di cura fondata sulla reciproca fiducia e sul mutuo rispetto dei valori e dei diritti e su un'informazione comprensibile e completa, considerando il tempo della comunicazione quale tempo di cura».

94. Questa esigenza trova un chiaro riscontro nell'art. 5, primo comma, della legge n. 219/2017, che disciplina la "pianificazione condivisa delle cure", stabilendo che, nell'ambito del rapporto di fiducia che deve caratterizzare la relazione tra medico e paziente, «rispetto all'evolversi delle conseguenze di una patologia cronica e invalidante o caratterizzata da inarrestabile evoluzione con prognosi infausta, può essere realizzata una pianificazione delle cure condivisa tra medico e paziente, alla quale il medico o l'equipe sanitaria sono tenuti ad attenersi qualora il paziente venga a trovarsi nella condizione di non poter esprimere il proprio consenso o in una condizione di incapacità».

95. Così MITTELSTADT 2021, p. 46.

96. Impegnando il medico, come ricordato *supra* (par. 3), ad «adeguare[re] la comunicazione alla capacità di comprensione della persona assistita o del suo rappresentante legale, corrispondendo a ogni richiesta di chiarimento».

97. In tema v., per tutti, KERASIDOU 2020.

98. Anche in questo ambito – come si è riscontrato per il consenso informato – all'interno del codice deontologico, ad una disciplina di carattere generale si affiancano richiami all'istituto all'interno di situazioni specifiche: così, ad esempio, nell'art. 43, dedicato all'interruzione volontaria di gravidanza, si ribadiscono i «doveri inerenti alla relazione di cura nei confronti della donna» che gravano anche sul medico obiettore di coscienza, mentre nell'art. 44, dedicato alla procreazione medicalmente assistita, si ribadiscono, anche in questo caso a carico del medico obiettore, i «doveri inerenti alla relazione di cura nei confronti della coppia».

La norma, per un verso, ripropone anche in questo caso l'impostazione propria della Convenzione di Oviedo, che colloca parimenti al centro della relazione tra il medico e paziente – configurata anche in quel contesto come “alleanza” – il mutuo riconoscimento di valori e diritti e la reciproca fiducia: si legge infatti nella relazione illustrativa alla Carta europea che «un fattore importante per il successo di un trattamento è la *fiducia* del paziente nel proprio medico. Questa fiducia determina anche i *doveri* del medico nei confronti del paziente. Un elemento importante di questi doveri è il rispetto dei *diritti* del paziente. Ciò crea e aumenta la *fiducia reciproca*. L'*alleanza terapeutica* si rafforzerà se i diritti del paziente saranno pienamente rispettati»⁹⁹; tra l'altro, la reciproca fiducia è posta al centro della relazione di cura anche dalla Carta europea di etica medica, che stabilisce, al *Principio 5*, che «il medico è confidente necessario del paziente. Tradisce questa *fiducia* se rivela ciò che ha appreso dal paziente». Per altro verso, innova rispetto al modello della Convenzione, sottolineando lo specifico rilievo detenuto, all'interno della relazione di cura, dalla comunicazione delle informazioni e ribadendo, anche sotto questo profilo, il nesso che collega l'istituto in esame con il dovere di informazione (e, di riflesso, con il consenso informato); si noti, inoltre, come nel testo trovi conferma anche la necessità che l'informazione offerta al paziente presenti le due caratteristiche fondamentali che si sono dianzi evidenziate, e cioè che sia «comprensibile e completa».

4.1. La centralità della visita medica e il ruolo dei dati nelle valutazioni cliniche

Con specifico riguardo all'impatto dell'intelligenza artificiale nella relazione di cura, gli indirizzi applicativi dell'art. 78 del codice di deontologia medica contengono diverse indicazioni rilevanti. Anzitutto, la relazione di cura viene evocata espressamente con riferimento al profilo temporale: sulla

scorta, infatti, del succitato art. 20, che invita a considerare «il tempo della comunicazione quale tempo di cura», l'indirizzo applicativo n. 2 impegna il medico a garantire, nell'uso delle tecnologie informatiche, «il recupero del *tempo* necessario per la relazione di cura». All'attenzione per il dato temporale si accompagna analoga considerazione per la dimensione, in senso lato, “spaziale” della relazione di cura, stabilendo che «il medico, facendo uso dei sistemi telematici, non può sostituire la visita medica che si sostanzia nella relazione diretta con il paziente, con una relazione esclusivamente virtuale» (indirizzo applicativo n. 6).

Il divieto di instaurare una relazione “esclusivamente virtuale” vuole ovviamente privilegiare anzitutto la compresenza di medico e paziente nello stesso luogo. Ciò comporta, per un verso, una limitazione al ricorso alla telemedicina, la quale, per sua natura, si sostanzia nell'erogazione di prestazioni sanitarie attraverso tecnologie che sviluppano la relazione medico-paziente senza necessità di compresenza fisica: l'indirizzo applicativo in esame prosegue infatti stabilendo che il medico può «utilizzare gli strumenti di telemedicina per le attività di rilevazione, o monitoraggio a distanza, dei parametri biologici e di sorveglianza clinica»; potremmo dire, in questa prospettiva, che può utilizzarle “soltanto” per le attività indicate (o “prevalentemente” per le attività indicate) e non, di norma, in sostituzione della visita medica tradizionale¹⁰⁰.

Naturalmente non si vuole disconoscere il ruolo decisivo svolto dalle diverse forme di assistenza da remoto, in particolare nelle situazioni di difficoltà o di emergenza sanitaria: segnatamente, durante la pandemia da Covid-19, la telemedicina ha rappresentato un'efficace “soluzione tampone” per sopperire alla «inadeguata implementazione della medicina di prossimità»¹⁰¹; e comunque ha consentito di potenziare l'assistenza territoriale e domiciliare – soprattutto a beneficio dei pazienti fragili e a mobilità limitata – e di ridurre l'ospedalizzazione¹⁰².

99. Così MITTELSTADT 2021, pp. 25-26.

100. Tra l'altro, il successivo indirizzo applicativo n. 13 precisa che «in ogni caso, il consulto e le consulenze mediante tecnologie informatiche della comunicazione “a distanza” devono rispettare tutte le norme deontologiche che regolano la relazione medico-persona assistita».

101. Così MORANA-BALDUZZI-MORGANTI 2022, p. 130.

102. *Ibidem*, le Autrici osservano tuttavia che il ricorso alla telemedicina non deve costituire un alibi per ritardare l'applicazione del decreto ministeriale 23 maggio 2022, n. 77 (adottato in attuazione del PNRR), che richiede

Per altro verso, la compresenza di medico e paziente nello stesso luogo, specialmente quando il luogo è quello del paziente, è particolarmente utile per identificare un insieme rilevante di fattori che incidono sulla salute dell'assistito: lo ricorda espressamente, in questo caso, la Carta europea di etica medica, che al *Principio 4* invita il medico a «considera[re] l'ambiente nel quale il paziente vive e lavora quale fondamentale determinante della sua salute».

L'elemento centrale della disciplina codicistica in argomento è dunque rappresentato dal ruolo primario e ineludibile – anche a fronte di un crescente ricorso alle nuove tecnologie informatiche – della visita medica “in presenza”, intesa in senso tradizionale. Centralità della visita medica che significa a sua volta centralità del contatto umano tra medico e paziente: come hanno sottolineato efficacemente in proposito il Comitato Nazionale per la Bioetica e il Comitato Nazionale per la Bioetica, le Biotecnologie e le Scienze della vita, «il contatto personale costituisce l'elemento essenziale di ogni diagnosi e di ogni terapia»¹⁰³. La macchina, infatti, per quanto intelligente, non può sostituire il medico nella «dimensione comunicativa, umana e fiduciaria» che questi instaura col paziente nell'ambito di una relazione diretta fra i due soggetti¹⁰⁴. Da questo punto di vista, occorre guardare con grande attenzione – e prudenza – alle applicazioni di elaborazione del linguaggio naturale che consentiranno, in futuro, di far gestire da un *artificial conversational agent* – in parte o interamente – il contatto iniziale con l'assistito o persino il triage (trattandosi, in quest'ultima ipotesi, di un'attività diagnostica in grado di decidere, nei casi più gravi, della stessa sopravvivenza del paziente)¹⁰⁵.

La visita medica si connota inoltre per la possibilità – ad oggi irrealizzabile attraverso le macchine – di sviluppare con il paziente una relazione

empatica: cioè – come dianzi sottolineato – uno dei principali elementi sui quali si costruisce il rapporto di fiducia tra medico e paziente e, dunque, sul quale si fonda la relazione di cura¹⁰⁶.

A questo proposito, può essere utile ricordare che il Consiglio d'Europa, nel delineare i cambiamenti indotti dall'intelligenza artificiale sui mezzi di erogazione dell'assistenza sanitaria, osserva che il progressivo spostamento di competenze e responsabilità assistenziali dall'uomo alla macchina produrrà un impatto sulla relazione medico-paziente (e sui diritti umani coinvolti in tale relazione) destinato a manifestarsi su sei diversi livelli. I primi tre rimandano all'ampia tematica dell'eguaglianza, già affrontata nelle pagine precedenti: diseguaglianza nell'accesso all'assistenza sanitaria di alta qualità e rischio di generare nuove diseguaglianze sanitarie nei Paesi membri; rischio di accentuare i pregiudizi sociali; insorgenza di *bias* legati all'automazione e dequalificazione conseguente al trasferimento delle responsabilità di cura. Si evocano quindi due tematiche altrettanto note: l'impatto sul diritto alla privacy e la trasparenza nei confronti degli operatori sanitari e dei pazienti (anch'essa in parte richiamata nelle pagine che precedono).

Il sesto e ultimo livello introduce invece una prospettiva in parte inedita, accennando alla alterazione del “resoconto del benessere” del paziente (*dilution of the patient's account of well-being*)¹⁰⁷. L'espressione coglie un aspetto essenziale del rapporto medico-paziente e segnala come l'AI, anche quando non sostituisca integralmente il medico, sia in grado di incidere in profondità sulla natura e sui contenuti dell'attività diagnostica e più in generale sulla qualità della relazione di cura. Il progressivo diffondersi delle tecnologie informatiche non si tradurrà infatti solo in una riduzione delle interazioni “faccia a faccia” tra medico e assistito;

di rafforzare la capacità del SSN di «operare come un sistema vicino alla comunità, progettato per le persone e con le persone».

103. COMITATO NAZIONALE PER LA BIOETICA E COMITATO NAZIONALE PER LA BIOSICUREZZA, LE BIOTECNOLOGIE E LE SCIENZE DELLA VITA 2020, p. 10.

104. Così BIANCARDO 2021, p. 115.

105. Così MITTELSTADT 2021, p. 8. Il Consiglio d'Europa richiama in proposito il potenziale utilizzo a tale scopo di GPT-3 di OpenAI.

106. Cfr. sul tema PERFRANCESCHI-PROCURANTI 2012, p. 73 ss.

107. Così MITTELSTADT 2021, p. 4.

il problema che appare ad oggi più rilevante è che, anche quando l'interazione continui a svolgersi "in presenza", le valutazioni cliniche sembrano destinate a basarsi sempre di più su rappresentazioni di dati (che saranno costruite a loro volta sempre di più mediante tecnologie di monitoraggio remoto, come ad esempio "app" sanitarie o orologi intelligenti)¹⁰⁸.

Questa tendenza – osserva il Consiglio d'Europa – induce (e sempre più indurrà) medico e paziente a discutere della salute prevalentemente, se non esclusivamente, sulla base di quantità misurabili o in termini interpretabili dalla macchina¹⁰⁹. Di conseguenza, l'intelligenza artificiale induce (e sempre più indurrà) a trascurare elementi essenziali del benessere del paziente, come gli stati sociali, mentali ed emotivi¹¹⁰.

In sostanza – conclude sul punto il Consiglio d'Europa – l'AI, pur consentendo di trattare più pazienti, in modo più efficiente e con costi inferiori, mina le dimensioni "non meccaniche" della cura¹¹¹ e inibisce la "comprensione tacita" (*tacit understanding*) della salute e del benessere del paziente: un elemento, quest'ultimo, che rischia di compromettere, a lungo andare, il rapporto fiduciario posto alla base della relazione di cura¹¹².

Al contrario, la relazione medico-paziente basata sulla fiducia e sull'empatia richiede: che il paziente non sia visto solo come un numero (il che rinvia al tema della "disumanizzazione" dianzi evocata);

un'adeguata abilità nel rispondere in modo non verbale e attraverso un dialogo condotto con competenza e sensibilità (*skilful and sensitive dialogue*) (il che rinvia al tema dell'empatia)¹¹³; una "complicità morale" che le intelligenze artificiali non possono replicare (il che rinvia al tema della fiducia)¹¹⁴; la comprensione "contestuale" dei valori, della storia e delle preoccupazioni del paziente (il che rinvia al tema della scarsa attenzione per gli stati sociali, mentali ed emotivi dell'assistito)¹¹⁵.

La mediazione tecnologica del trattamento medico determina invece una "decontestualizzazione" della condizione del paziente¹¹⁶, che induce a trascurare non solo le condizioni mentali ed emotive che incidono sullo stato di salute, ma anche, più in generale, le condizioni sociali ed ambientali in senso lato, che contribuiscono a determinare il benessere complessivo dell'assistito.

Alla luce di quanto lo stesso Consiglio d'Europa sostiene, non si può allora condividere l'affermazione contenuta nel documento in esame per cui l'intelligenza artificiale non incide «né sul ruolo dell'assistito, né sui fattori che spingono a rivolgersi al medico, né sulla vulnerabilità del paziente»¹¹⁷: il ruolo del paziente, infatti, risulta modificato dalla crescente disponibilità di informazioni sul proprio stato di salute, nonché su ipotesi diagnostiche e percorsi terapeutici che l'assistito è in grado di acquisire autonomamente, emancipandosi in parte dalla dipendenza informativa nei confronti del

108. *Ivi*, p. 51.

109. *Ivi*, p. 6.

110. *Ivi*, p. 52. In coerenza, peraltro, con l'orientamento espresso dall'Organizzazione Mondiale della Sanità, che ha definito il concetto di salute come «una condizione di completo benessere fisico, mentale e sociale e non esclusivamente l'assenza di malattia o infermità»: così il Preambolo alla costituzione dell'OMS come adottato dalla Conferenza Internazionale della Sanità, New York, 19-22 giugno 1946, sottoscritto il 22 luglio 1946 ed entrato in vigore il 7 aprile 1948 (cfr. *Official Records of the World Health Organization*, n. 2, 100).

111. *Ivi*, p. 43.

112. *Ivi*, p. 6.

113. *Ivi*, p. 39. La *skinfulness* del medico, in particolare, può manifestarsi sia nella "perizia" (o, per l'appunto, nella competenza), sia anche nella "abilità", che è richiesta all'operatore sanitario al fine di persuadere il paziente dell'opportunità di sottoporsi ad un determinato intervento diagnostico o terapeutico: sul legame tra "consenso" e "persuasione", con un suggestivo richiamo agli spunti che possono farsi risalire fino alle *Leggi* di Platone, cfr. GRASSO 2011, p. 2 ss.

114. *Ivi*, p. 43.

115. *Ivi*, p. 51.

116. *Ivi*, p. 52.

117. *Ivi*, p. 4.

medico¹¹⁸; i cennati mutamenti che vanno interessando l'asimmetria informativa tra medico e paziente incidono a loro volta sui fattori che spingono l'assistito a rivolgersi al medico, determinando, a seconda dei casi, un aumento delle richieste dovute ad auto-diagnosi prive di fondamento o ad una diminuzione delle richieste dovute ad altrettanto dannose auto-prescrizioni (oltre al significativo aumento di persone che preferiscono rivolgersi ai medici "virtuali" nelle forme più diverse)¹¹⁹; la vulnerabilità dell'assistito risulta incisa perché un paziente meno "compreso" nel suo contesto, sia emotivo che sociale, è un paziente più debole.

Appare invece più condivisibile l'impostazione che distingue l'impatto dell'intelligenza artificiale sulla relazione di cura in base al modello di servizio adottato¹²⁰: così, se l'AI viene utilizzata per *integrare* le competenze degli operatori sanitari, l'impatto sulla relazione di cura è minore¹²¹. Se l'AI viene impiegata per *aumentare* (*heavily augment*) o *sostituire* le competenze degli operatori sanitari, l'impatto sulla relazione di cura è «difficile da prevedere»¹²².

4.2. Il mutamento del ruolo del medico conseguente alla trasformazione della relazione di cura in un rapporto trilatero

Lo scenario che vede la diagnosi e la cura dei pazienti totalmente affidata a sistemi artificiali, con una conseguente riconfigurazione radicale della relazione medico-assistito, appare ancora lontano.

Tuttavia, un cambiamento è già in atto: la relazione medico-paziente va infatti progressivamente trasformandosi in una relazione medico-paziente-intelligenza artificiale¹²³.

Questo processo verosimilmente produrrà nel tempo una mutazione del ruolo del medico, che appare suscettibile di condurre a diversi esiti. Potrebbe infatti portare: ad un medico "intermediario" tra la macchina e il paziente¹²⁴; ad un medico "al servizio" della macchina¹²⁵ o anche ad un medico "vittima" della macchina, qualora quest'ultima favorisse il diffondersi di pazienti "potenziati", rompendo l'equilibrio asimmetrico sul quale si è tradizionalmente fondato il rapporto medico-paziente¹²⁶.

La tecnologia, infatti, incide sui "rapporti di forza" che operano all'interno della relazione tra il medico e il paziente (dei quali, va ricordato, il codice deontologico all'art. 20 ribadisce la reciproca autonomia). Ad esempio, come prima si rammentava¹²⁷, la rete Internet offre ai pazienti un maggiore accesso alle informazioni mediche¹²⁸: questo fenomeno – oltre ai rischi legati all'acquisizione di informazioni fuorvianti – fa emergere la figura di un paziente sempre più "esperto" (o, meglio, sempre più convinto di essere esperto), che erode la posizione del medico come soggetto competente¹²⁹; ma, in prospettiva, le intelligenze artificiali saranno in grado di offrire informazioni mediche più dettagliate e più "personalizzate" direttamente al paziente, aumentando lo squilibrio. Oltre a ciò, la figura di un

118. Sul punto cfr. anche *infra*, par. 4.2, le osservazioni nel testo in merito al paziente "potenziato".

119. In argomento, con specifico riferimento all'impatto derivante dal crescente ricorso, anche a in questo ambito, a strumenti di intelligenza artificiale generativa, cfr. IFTIKHAR–FERAS IFTIKHAR–IFTIKHAR HANIF 2023.

120. MITTELSTADT 2021, p. 7.

121. Il Consiglio d'Europa parla in realtà di impatto "minimo" – ma la posizione è criticabile alla luce delle osservazioni formulate *supra* – aggiungendo che il "modello ideale" corrisponderebbe a quello di un'intelligenza artificiale che utilizzi i migliori aspetti della competenza clinica umana e della capacità di elaborazione dei dati a fini diagnostici realizzabile attraverso le tecnologie informatiche più avanzate.

122. *Ibidem* (così come sarebbe imprevedibile l'impatto sulla disegualianza nell'accesso alle cure: cfr. *ivi*, p. 45).

123. In argomento si v. le considerazioni sviluppate in MITTELSTADT 2021, p. 7 ss.

124. Come accennato *supra*, par. 3.2.

125. Questo timore appare molto diffuso nella classe medica: sul punto si v. ad es. PANTI 2022.

126. I rischi legati alla progressiva emersione di pazienti "potenziati" sono illustrati da EMANUEL–EMANUEL 1992, p. 2221 ss.

127. Cfr. par. 4.1.

128. Sul tema si v., *ex multis*, DIAZ–GRIFFITH–NG et al. 2002.

129. *Ibidem*.

medico “vittima” della macchina va emergendo in relazione soprattutto al fenomeno della “cattura” del sistema informatico rispetto all’operatore, sempre più indotto a non contraddire la soluzione suggerita dall’algoritmo, affidandosi totalmente alle indicazioni provenienti dall’AI¹³⁰.

Di fronte ai rischi richiamati, emerge con forza l’esigenza di stabilire al più presto – come ha opportunamente suggerito il Consiglio d’Europa – “standard e requisiti solidi” (*robust standards and requirements*) per fronteggiare il nuovo tipo di relazione di cura che si va affermando a seguito dell’evoluzione tecnologica in corso¹³¹.

Il richiamo operato dal Consiglio d’Europa agli standard coglie una questione giuridica fondamentale, che è costituita dall’impatto dei sistemi di AI sugli standard professionali al cui rispetto richiama l’art. 4 della Convenzione di Oviedo¹³²: questione peraltro delicatissima, perché impone di affrontare il problema – giuridicamente diabolico – della *soggettività* della macchina.

In proposito il Consiglio d’Europa avanza qualche primo suggerimento: ad esempio, osserva che, nel caso in cui le AI interagiscano direttamente con i pazienti, tali sistemi dovrebbero identificarsi come sistemi artificiali¹³³, anche per non minare la fiducia che il paziente ripone nel medico. Ma, soprattutto, invita a riflettere su una circostanza fondamentale: non è chiaro, infatti (e la questione merita naturalmente di essere risolta al più presto) se gli standard professionali richiamati dalla

Convenzione, nel caso in cui l’intervento medico sia operato direttamente da un sistema artificiale, vincolino allo stesso modo e nella stessa misura gli sviluppatori, i produttori o i fornitori di sistemi di AI impiegati in ambito sanitario¹³⁴. Sul punto, vale ricordare che la relazione esplicativa alla Convenzione di Oviedo stabilisce che gli “standard professionali” di cui all’art. 4 riguardano soltanto «gli operatori sanitari chiamati a compiere atti medici». In questa prospettiva, un chatbot progettato per gestire il triage dei pazienti può considerarsi un “operatore sanitario” che compie un “atto medico”? L’interrogativo rinvia inevitabilmente alla questione della soggettività dell’intelligenza artificiale, e, nel caso specifico, alla possibilità di considerare il chatbot come un “operatore sanitario”¹³⁵.

Certo, ad oggi il grado di autonomia che i sistemi di AI sono in grado di raggiungere – e, soprattutto, i vincoli giuridici imposti al loro utilizzo, che non consentono di affidare totalmente a sistemi artificiali l’attività di cura¹³⁶ – ci inducono a considerare come una potenziale violazione degli standard professionali di cui all’art. 4 della Convenzione di Oviedo qualsiasi carenza nella supervisione dell’intelligenza artificiale da parte di operatori sanitari¹³⁷. Volgendo tuttavia lo sguardo al tempo futuro, merita di essere valutato con grande attenzione il monito del Consiglio d’Europa, che suggerisce estrema cautela nell’incorporare sistemi di AI che interagiscono direttamente col paziente nei

130. In argomento si v., per tutti, SIMONCINI 2019, p. 81 ss.

131. Così MITTELSTADT 2021, p. 65.

132. Articolo 4 (*Obblighi professionali e regole di condotta*). Ogni intervento nel campo della salute, compresa la ricerca, deve essere effettuato nel rispetto delle norme e degli obblighi professionali, così come nel rispetto delle regole di condotta applicabili nella fattispecie.

133. MITTELSTADT 2021, pp. 5 e 46.

134. *Ivi*, p. 45.

135. *Ibidem*.

136. Si consideri a riguardo che l’AI Act classifica i sistemi di intelligenza artificiale utilizzati nell’erogazione di servizi pubblici e privati essenziali (nei quali rientra, a pieno titolo, l’assistenza sanitaria) come sistemi “ad alto rischio”, rispetto ai quali va sempre garantita la supervisione umana. In proposito, si v. in particolare l’art. 10, par. 3, che prescrive la pertinenza, la rappresentatività, l’assenza di errori e la completezza dei dati di addestramento, convalida e prova utilizzati nei sistemi ad alto rischio. Per una panoramica della disciplina contenuta nel progetto di AI Act con riguardo all’uso di sistemi di intelligenza artificiale in medicina, si v., *ex multis*, QUARANTA-AMANTEA-GROSSO 2023, e MESZAROS-MINARI-HUYS 2002.

137. Cfr. in proposito MITTELSTADT 2021, p. 45.

protocolli operativi di professioni sanitarie vincolate da standard professionali¹³⁸.

5. Nota conclusiva: il “rispetto della persona umana” come *primato dell’uomo sulla macchina*?

Emerge dall’analisi svolta un ruolo del medico nella relazione di cura che valga a garantire non soltanto il “contatto umano” (e i benefici connessi in termini di empatia, fiducia, efficacia della diagnosi, valutazione del benessere complessivo del paziente, compliance terapeutica), ma anche il “controllo umano” sulla macchina: la supervisione dell’uomo sul sistema di AI, anche per evitare la “cattura” della decisione¹³⁹.

E allora vale la pena, in conclusione, di riprendere lo spunto contenuto nell’art. 6 del codice di deontologia medica, che al secondo comma impegna il medico, «in ogni ambito operativo», a perseguire «l’uso ottimale delle risorse pubbliche e private salvaguardando l’efficacia, la sicurezza e l’umanizzazione dei servizi sanitari». Va ricordato, infatti, ancora una volta, che la relazione di cura deve riflettere il necessario «rispetto della persona umana», richiamato dall’art. 32 Cost., secondo comma, con espresso riferimento ai trattamenti sanitari obbligatori, ma che risulta

«estensibile anche ai trattamenti volontari»¹⁴⁰ e può quindi considerarsi un vincolo imposto (esplicitamente o implicitamente) a tutti i trattamenti sanitari¹⁴¹.

Ribadire la centralità della persona umana nella pratica medica è tanto più necessario quanto più l’affidamento a sistemi automatici dotati di margini sempre maggiori di autonomia rischia di “disumanizzare” il rapporto con il paziente (facendo emergere la profonda contraddizione che accompagna l’impiego di sistemi di AI in medicina, che rende la cura, per un verso, sempre più “personalizzata” nella modulazione delle terapie e, per altro verso, più “spersonalizzante” nello svolgimento della relazione medico-paziente).

Riguardato in questa prospettiva, il «rispetto della persona umana» dell’art. 32 della Costituzione potrebbe allora postulare anche una priorità della persona umana rispetto alla macchina¹⁴², da garantire in particolare all’interno di una relazione medico-paziente che è – e deve rimanere – anche alla luce di questo fondamentale valore costituzionale, una relazione fra due persone, all’interno della quale, in futuro, forse dovremo occuparci di tutelare non solo la persona del malato, ma anche la persona del medico.

Riferimenti bibliografici

138. *Ibidem*.

139. Cfr. *supra*, par. 4.2, spec. nt. 130. Non a caso il Consiglio d’Europa mette in evidenza i rischi che si manifestino i c.d. “*bias* da automazione”, cioè la tendenza a fidarsi dei risultati suggeriti dai sistemi automatici in base alla loro oggettività e accuratezza *percepita* (MITTELSTADT 2021, pp. 20 e 57: un fenomeno, nota il documento, osservato in particolare all’interno delle burocrazie con ridotto senso di responsabilità personale e di fronte all’esecuzione di azioni altrimenti ingiustificabili).

140. Così MORANA–BALDUZZI–MORGANTI 2022, p. 131.

141. La centralità della persona umana nella pratica medica trova significative conferme sia nella legislazione ordinaria, sia nella giurisprudenza costituzionale. In ordine al primo profilo, basti ricordare nuovamente l’art. 1, secondo comma, della legge n. 833/1978 (già richiamato al par. 3), che viene in rilievo, in questa sede, per il richiamo alla dignità della persona umana il cui rispetto costituisce un limite fondamentale dell’attività di tutela della salute fisica e psichica. Quanto alla giurisprudenza costituzionale, può richiamarsi in proposito la sentenza n. 282 del 2002, in cui si sottolinea come il rispetto della persona umana integri il concetto di “appropriatezza” della pratica terapeutica, che è appropriata se garantisce il «rispetto della integrità psico-fisica e della personalità del malato nell’attività di cura» (punto 3 considerato in diritto).

142. In linea, peraltro, con il “primato” della persona umana sancito dalla Convenzione di Oviedo, che all’art. 2 (Primato dell’essere umano), recita: «l’interesse e il bene dell’essere umano debbono prevalere sul solo interesse della società o della scienza».

- AA.VV. (2020), *L'intelligenza artificiale per prevenire il cancro al colon retto*, in "Sanità digitale", 16 novembre 2020
- A.S. ADAMSON, A. SMITH (2018), *Machine Learning and Health Care Disparities in Dermatology*, in "JAMA Dermatology", 2018, n. 11
- A. ALIPER, R. KUDRIN, D. POLYKOVSKIY et al. (2023), *Prediction of Clinical Trials Outcomes Based on Target Choice and Clinical Trial Design with Multi-Modal Artificial Intelligence*, in "Clinical Pharmacology & Therapeutics", 2023, n. 5
- R. BALDUZZI, D. PARIS (2008), *Corte costituzionale e consenso informato tra diritti fondamentali e ripartizione delle competenze legislative*, in "Giurisprudenza costituzionale", 2008
- G. BEDI, F. CARRILLO, G. CECCHI et al. (2015), *Automated analysis of free speech predicts psychosis onset in high-risk youths*, in "NPJ Schizophrenia", 2015, n. 1
- A. BIANCARDO (2021), *Problematiche etico-giuridiche relative all'utilizzo dell'intelligenza artificiale in ambito sanitario*, in "Jus-online", 2021, n. 3
- A. BIANCARDO (2018), *I reati informatici*, Esc Service, 2018
- C. CASONATO (2019), *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in "Diritto pubblico comparato ed europeo", 2019, numero speciale
- G. CATTANEO (1957), *Il consenso del paziente al trattamento medico-chirurgico*, in "Rivista trimestrale di diritto e procedura civile", 1957
- L. CHENXI, J. DIAN, L. ZHE (2020), *Artificial Intelligence (AI)-aided Disease Prediction*, in "BIO Integration", 2020, n. 3
- COMITATO NAZIONALE PER LA BIOETICA (2008), *La sperimentazione farmacologica sulle donne*, 28 novembre 2008
- COMITATO NAZIONALE PER LA BIOETICA E COMITATO NAZIONALE PER LA BIOSICUREZZA, LE BIOTECNOLOGIE E LE SCIENZE DELLA VITA (2020), *Intelligenza artificiale e medicina: aspetti etici*, 20 maggio 2020
- CONSIGLIO SUPERIORE DI SANITÀ (2021), *I sistemi di intelligenza artificiale come strumento di supporto alla diagnostica*, 9 novembre 2021
- A. DI MARTINO (2024), *Il consenso trasparente (e non solo informato) nell'età degli algoritmi: qualche chiarimento dalla Cassazione*, in "Osservatorio sullo Stato digitale IRPA", 7 febbraio 2024
- J.A. DIAZ, R.A. GRIFFITH, J.J. NG et al. (2002), *Patients' Use of the Internet for Medical Information*, in "Journal of General Internal Medicine", 2002, n. 3
- E.J. EMANUEL, L.L. EMANUEL (1992), *Four Models of the Physician-Patient Relationship*, in "JAMA - The Journal of the American Medical Association", vol. 267, 1992, n. 16
- A. ESTEVA, B. KUPREL, R. NOVOA et al. (2017), *Dermatologist-level classification of skin cancer with deep neural networks*, in "Nature", vol. 542, 2017
- J.M. FELDMAN, K. KUCK, T. HEMMERLING (2012), *Black Box, Gray Box, Clear Box? How Well Must We Understand Monitoring Devices?*, in "Anesthesia & Analgesia", 2012, n. 6
- G. GRASSO (2011), *Consenso informato, libertà di scelta e disponibilità del proprio corpo*, in "Forum di Quaderni Costituzionali", 2011, ora in G. Cocco (a cura di), "Lo Statuto giuridico delle informazioni", Atti del Convegno di Milano, Università Bicocca, 24 maggio 2010, Giuffrè, 2012
- L. IFTIKHAR, M. FERAS IFTIKHAR, M. IFTIKHAR HANIF (2023), *DocGPT: Impact of ChatGPT-3 on Health Services as a Virtual Doctor*, in "EC Paediatrics", 2023, n. 3

- L. KANG YOON, K. JUNHEWK (2016), *Artificial Intelligence Technology Trends and IBM Watson References in the Medical Field*, in “Korean Medical Education Review”, 2016, n. 2
- A. KERASIDOU (2020), *Artificial intelligence and the ongoing need for empathy, compassion and trust in healthcare*, in “Bulletin of the World Health Organization”, 2020, n. 1
- S. MAJUMDER, T. MONDAL, M.J. DEEN (2017), *Wearable Sensors for Remote Health Monitoring*, in “Sensors”, 2017, n. 1
- A. MALVA, V. ZURLO (2019), *Babylon Health: il servizio anglosassone di Medicina Generale privato basato su app*, in “Rivista Società Italiana di Medicina Generale”, 2019, n. 5
- J. MESZAROS, J. MINARI, I. HUYS (2002), *The future regulation of artificial intelligence systems in healthcare services and medical research in the European Union*, in “Frontiers in Genetics”, 2002, n. 4
- B. MITTELSTADT (2021), *The impact of Artificial Intelligence on the doctor-patient relationship*, Council of Europe, December 2021
- D. MORANA (2021), *La salute come diritto costituzionale*, Giappichelli, 2021
- D. MORANA, T. BALDUZZI, F. MORGANTI (2022), *La salute “intelligente”: eHealth, consenso informato e principio di non-discriminazione*, in “federalismi.it”, 28 dicembre 2022
- A. PANTI (2022), *La deontologia all'alba dell'intelligenza artificiale*, in “il punto - confronti su medicina e sanità”, 19 dicembre 2022
- S. PENASA (2007), *Alla ricerca dell'anello mancante: il deposito dello strumento di ratifica della Convenzione di Oviedo*, in “Forum di Quaderni costituzionali”, 2007
- L. PERFRANCESCHI, L. PROCURANTI (2012), *Ascolto ed empatia: riflessioni sulla costruzione della relazione di cura*, in A. Moretto (a cura di), “Il paziente tra coscienza e relazionalità”, Cortina, 2012
- P. PHAN, S. MITRAGOTRI, Z. ZHAO (2023), *Digital therapeutics in the clinic*, in “Bioengineering and Translational Medicine”, 2023, n. 4
- M. QUARANTA, I.A. AMANTEA, M. GROSSO (2023), *Obligation for AI Systems in Healthcare: Prepare for Trouble and Make it Double?*, in “The Review of Socionetwork Strategies”, vol. 17, 2023
- G. RESTA (2019), *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in “Politica del diritto”, 2019, n. 2
- A. SAINI (2017), *Inferiori. Come la scienza ha penalizzato le donne*, HarperCollins, 2017
- L. SHANA (2020), *The Geographic Bias in Medical AI Tools. Ethics and Justice, Healthcare, Machine Learning*, in “Stanford University Human-Centered Artificial Intelligence News and Announcements”, 21 September 2020
- A. SIMONCINI (2019), *L'algoritmo incostituzionale: intelligenza artificiale e futuro delle libertà*, in “Biolaw journal – Rivista di BioDiritto”, 2019, n. 1
- E. STRICKLAND (2019), *IBM Watson, heal thyself: How IBM overpromised and underdelivered on AI health care*, in “IEEE Spectrum”, 2019, n. 4
- M. SUN, T. OLIWA, M.E. PEEK et al. (2022), *Negative Patient Descriptors: Documenting Racial Bias in the Electronic Health Record*, in “Health Affairs”, 2022, n. 2
- K. WARWICK (2020), *Superhuman Enhancements via Implants: Beyond the Human Mind*, in Philosophies, 2020, n. 5 (special issue on *Human Enhancement Technologies and Our Merger with Machines*)
- WORLD HEALTH ORGANIZATION (2023), *Regulatory considerations on artificial intelligence for health*, by Dr. J. Farrar, Chief Scientist, W.H.O., 2023
- WORLD HEALTH ORGANIZATION (2012), *Legal frameworks for eHealth*, 2012

- G.-Z. YANG, J. CAMBIAS, K. CLEARY et al. (2017), Medical robotics – Regulatory, ethical, and legal considerations for increasing levels of autonomy, in “Science Robotics”, 2017
- X. ZHANG, Z. MA, H. ZHENG et al. (2020), The combination of brain-computer interfaces and artificial intelligence: applications and challenges, in “Annals of Translational Medicine”, 2020, n. 8
- P. ZUDDAS (2020), Brevi note sulla trasparenza algoritmica, in “Amministrazione in cammino”, 2020, vol. 1, 5 giugno 2020
- P. ZUDDAS (2020A), Intelligenza artificiale e discriminazioni, in Aa.Vv., “Liber amicorum per Pasquale Costanzo - Diritto costituzionale in trasformazione”, I, Costituzionalismo, Reti e Intelligenza artificiale, in “Consulta OnLine”, 2020
- P. ZUDDAS (2019), *La pari dignità sociale a tre dimensioni. Posizione, giudizio, trattamento*, Wolters Kluwer-Cedam, 2019
- F. ZUIDERVEEN BORGESIUUS (2018), Discrimination, Artificial Intelligence and Algorithmic Decision-Making, Council of Europe, 2018



TONINO CANTELMi – LUISA LODEVOLE

Nuove prassi e norme per un sistema sanitario “smart”: ricadute dell’AI Act sulla relazione di cura

L'articolo si propone di esplorare lo stato dell'arte dell'utilizzo dei sistemi di IA nel settore sanitario, in particolare sotto forma di software per il processo decisionale clinico e di dispositivi medici. Gli autori assumono una duplice prospettiva: da un lato, quella del giurista che rileva le implicazioni pratiche delle applicazioni dell'IA nella cura e nella promozione della salute umana e raccomanda l'adozione di una normativa o valuta quella adottata, in questo caso il recente regolamento emanato dall'Unione europea. Dall'altro lato, viene assunto il punto di vista della scienza medica che, unito alla riflessione bioetica, evidenzia gli effetti di ritorno sulla visione della vita dell'uomo postmoderno.

Intelligenza artificiale – Sistema sanitario – Coscienza – Scientismo – Fiducia

New practices and standards for a ‘smart’ healthcare system: impact of the AI Act on the care relationship

The paper aims to explore the state of the art of the use of AI systems in the healthcare sector, particularly in the form of software for clinical decision-making and medical devices. The authors take a twofold perspective: on the one hand, that of the jurist who notes the practical implications of AI applications in the treatment and promotion of human health and recommends the adoption of a regulation or evaluates the one adopted, in this case, the recent Regulation issued by the European Union. On the other hand, the point of view of medical science is taken, which, combined with bioethical reflection, highlights the feedback effects on post-modern man's view of life.

Artificial intelligence – Healthcare – Consciousness – Scientism – Trust

T. Cantelmi è professore associato all'Istituto di Psicologia, Università Gregoriana – Roma e membro del Comitato Nazionale per la Bioetica, Gruppo di lavoro “Tecnologie emergenti”

L. Lodevole è ricercatrice presso il Dipartimento di Giurisprudenza, Università degli Studi di Roma Tor Vergata

L'articolo è stato concepito e sviluppato in modo condiviso dagli autori. Mentre i paragrafi 1 e 10 sono riferibili ad entrambi, Tonino Cantelmi è autore dei paragrafi nn. 2, 3, 4 e 5; Luisa Lodevole è autore dei paragrafi nn. 6, 7, 8 e 9

SOMMARIO: 1. Introduzione: l’intelligenza artificiale: tra diritto e medicina. – 2. Circuiti elettronici e circuiti cerebrali. – 3. Neuroplasticità e *Intelligenza meccanica*. – 4. *Menti, cervelli ...* e coscienze. – 5. Il riduzionismo scienziato. – 6. Un modello normativo per i sistemi di IA. – 7. L’attività dei sistemi di IA sotto la lente del diritto: definizioni e classificazioni. – 8. Responsabilità per l’utilizzo dei sistemi di IA in ambito sanitario. – 8.1. *L’imputazione soggettiva: le figure coinvolte nella catena di valore dell’IA*. – 8.2. *La ricostruzione oggettiva: tra obblighi di trasparenza e explainability*. – 9. IA nel sistema sanitario: da ausilio ad ausiliario. – 10. *AI in healthcare*: un problema di fiducia.

1. Introduzione. L’intelligenza artificiale tra diritto e medicina

Dagli sviluppi della ricerca sull’Intelligenza artificiale¹ (d’ora in poi IA) non sembra impossibile che l’IA in futuro sostituisca il medico. Anzi, già oggi in alcune aree del mondo i pazienti preferiscono l’iscrizione in sistemi di assistenza sanitaria privati², digitalizzati e telematizzati, piuttosto che nei servizi sanitari offerti dall’amministrazione pubblica, in particolare il classico medico di medicina generale “in carne ed ossa”.

Le applicazioni dei sistemi di IA alle attività di cura e promozione della salute³ umana si sono

moltiplicate negli ultimi anni, così come sono sempre più numerosi gli studi sulle implicazioni deontologiche⁴ e bioetiche⁵ di questa prassi.

Gli utilizzi delle tecnologie quali ausilio del procedimento clinico, sia nel momento della formulazione della diagnosi⁶ che della prescrizione della terapia, oppure come strumento operativo nella chirurgia robotica⁷, sollevano questioni di carattere deontologico e biogiuridico⁸, nonché riflessioni antropologiche⁹ e bioetiche¹⁰.

Una prima questione riguarda la natura e finalità dell’atto medico e le sue leggi intrinseche. Una riflessione sulla specificità dell’arte medica permette di valutare in quali segmenti dell’attività

1. Per una trattazione del tema si veda AMATO MANGIAMELI 2023; AMATO MANGIAMELI 2022; AMATO MANGIAMELI 2022-A. Cfr. anche FINOCCHIARO 2022; FRANCESCHELLI 2023; GABRIELLI–RUFFOLO 2019; SARTOR 2022.
2. Cfr. l’app di servizi di medicina generale già notevolmente diffusa nel Regno Unito “Over 100,000 people already have GP at Hand as their NHS GP, with a 96% satisfaction score”, in [Babylon GP at hand](#).
3. Cfr. TOZZI 2023; nonché ALHASHMI–HASHEM–AL–QUDAH 2024; IQBAL–CORTÉS JAIMES–MAKINENI et al. 2023; KHERA–BUTTE–BERKWITS et al. 2023; PAREKH–SHAIKH–SIMRAN et al. 2023; XU–YANG–ARIKAWA–BAI 2023.
4. BALI–GARG–BALI 2019; BARRACCA–LEDDE–MANCOSU et al. 2017; HE–BAXTER–XU et al. 2019; MISHRA–SAVULESCU–GIUBILINI 2021; MUSACCHIO–GUAITA–OZZELLO et al. 2018.
5. DAVERIO–MACIOCE 2023; MORANA–BALDUZZI–MORGANTI 2022; PALAZZANI 2021. Cfr. anche FERIOLI 2019.
6. CONSIGLIO SUPERIORE DI SANITÀ 2021.
7. CONSIGLIO SUPERIORE DI SANITÀ 2023.
8. Cfr. nell’ambito del Consiglio d’Europa: COUNCIL OF EUROPE 1997; COUNCIL OF EUROPE 2020; MITTELSTADT 2022. Nel contesto delle Nazioni Unite: UNESCO 2021, UNESCO 2017, UNESCO 2005. Per l’Organizzazione Mondiale della Sanità: WORLD HEALTH ORGANIZATION 2021.
9. KAMPOWSKI 2010.
10. Cfr. il parere espresso da COMITATO NAZIONALE PER LA BIOETICA 2020. Per un inquadramento sistematico MAIER–SHIBLES 2011.

sanitaria l'utilizzo di sistemi di IA sia possibile e auspicabile e in quali non lo sia. Oltre a ciò, consentirebbe di individuare quali fasi eventualmente non possano essere delegate ad un sistema automatizzato, a pena di tradire la natura specifica della professionalità medica.

Un'altra questione emerge a causa del tipo di tecnologia: i sistemi di IA, software o robot¹¹, sollevano, rispetto a tutte le altre tecnologie informatiche e telematiche, dilemmi nuovi, derivanti dalle caratteristiche proprie di un agente intelligente, che non solo è in grado di pensare umanamente ma anche di agire razionalmente¹² e di continuare a modificare e riprogrammare se stesso attraverso l'apprendimento automatico.

L'ipotesi di macchine pensanti¹³ ha suscitato da lungo tempo linee di ricerca volte ad esplorare il funzionamento della mente umana¹⁴ e la riproducibilità del pensiero¹⁵: sul punto, sebbene le scienze neurologiche e cognitive abbiano analizzato le circonvoluzioni della massa cerebrale e scoperto alcune reazioni elettrochimiche dei suoi circuiti, allo stato attuale l'investigazione è appena agli inizi e non sembra che sia stata trovata la via d'uscita dal labirinto.

Un ulteriore interrogativo sorge a causa dell'intrusione di un ulteriore "agente" nell'interazione tra medico e paziente¹⁶, il sistema di IA, che, però, non è un mero *medium*, ma neanche un soggetto¹⁷. La mediazione di questo "terzo" in una relazione che è finora stata sempre "a due", potrebbe portare ad esiti, in una certa misura, imprevedibili: eppure, poiché l'arte medica si è in larga parte consolidata

in buone pratiche e linee guida, ci si chiede come questo elemento terzo possa essere incluso nei protocolli e nelle prassi cliniche o chirurgiche. D'altro canto, poiché quelle linee guida costituiscono il parametro di valutazione della diligenza¹⁸ del professionista – ben diversa dall'ordinaria diligenza del comune cittadino – il giurista deve risolvere due fondamentali *quaestiones*: quali siano i criteri di imputazione delle attività svolte dall'agente intelligente¹⁹; se siano applicabili, e in che modo, i regimi previsti dalle legislazioni nazionali in tema di responsabilità professionale in campo sanitario anche quando intervenga la mediazione dell'IA.

Il diritto, con le sue categorie rigide e fredde, non riesce a modulare il suo intervento in base alla diversa intensità di cooperazione dei differenti sistemi di IA: quindi risulta particolarmente difficile inquadrare l'IA con i modelli classici del diritto civile.

2. Circuiti elettronici e circuiti cerebrali

La ricerca sull'IA ha avuto origine dal tentativo di riprodurre il pensiero in macchine. Gli studiosi a partire dal XX secolo hanno mosso i primi passi su questa strada con diversi approcci.

Da un lato cercarono di osservare e descrivere cosa accade nel cervello umano quando pensa, con tecniche di indagine, c.d. *neuroimaging*, sempre più sofisticate, che ad oggi non hanno ancora esaurito tutte le questioni aperte.

Dall'altro lato, come prospettato da Turing, i ricercatori del settore hanno tentato di riprodurre le attività del cervello tramite ingranaggi o

11. Per una classificazione nelle due categorie di SIAP ovvero "Sistemi di IA Programmi" e SIAR "Sistemi di IA Robot", cfr. TADDEI ELMi 2020, in particolare p. 848.

12. Cfr. RUSSELL–NORVIG 2021, pp. 4-8.

13. TURING 1950.

14. Cfr. lo studio di SEARLE 1984.

15. Il binomio intelligenza artificiale fu utilizzato per la prima volta nel 1956, anno della *Proposal for the Dartmouth Summer Research Project on Artificial Intelligence* primo evento ufficialmente volto a riunire ricercatori su questa linea di ricerca, in particolare John McCarthy, Marvin Minsky, Claude Shannon e Nathaniel Rochester, cfr. MCCARTHY–MINSKY–ROCHESTER–SHANNON 2006. Gli studi di McCulloch e Pitts sul neurone artificiale e quelli di Turing sulle macchine pensanti sono da considerare prodromici rispetto all'incontro del 1956. Per le notizie storiche v. RUSSELL–NORVIG 2021, p. 19 ss.

16. HELZEL 2021.

17. Per una discussione sul punto cfr. SARTOR 2002 e SARTOR 2022, nonché TADDEI ELMi 2020.

18. CAMPIGLIO 2023; GRASSO 2023; nonché RUFFOLO 2021; RUFFOLO 2021-A.

19. LUCARELLI TONINI 2023; SALITO 2022; SALVATORE 2023.

meccanismi che potessero "lavorare" come il cervello, ovvero elaborare le informazioni in ingresso, sulla base di una tavola di istruzioni, allo stesso modo in cui le elabora la mente umana, fornendo gli stessi prodotti in uscita. La sfida per gli studiosi consisteva pertanto nell'arrivare a codificare una tavola di istruzioni tale che, inserita in un cervello elettronico, gli permettesse di funzionare e quindi di risolvere problemi allo stesso modo in cui li avrebbe risolti un uomo. Trovata la tavola di istruzioni, si sarebbe potuto dire di aver scoperto come funziona il cervello.

Si ricorda che il test di Turing era costruito come una prova *a contrario*: come il matematico esplicitamente affermava²⁰, egli stesso non era in grado di esporre argomenti sufficienti per fondare l'ipotesi che le macchine possono pensare, pertanto, la sua arringa a sostegno dei suoi argomenti era articolata come confutazione delle principali controdeduzioni a lui rivolte dalle controparti.

Di conseguenza, come evidenziato da Searle²¹, anche nel caso in cui la macchina riuscisse ad ingannare l'interrogante²² – il quale non fosse in grado di distinguere quale risposta al suo quesito provenisse da un uomo e quale da una macchina – la prova di Turing non dimostrava affatto che la macchina potesse pensare, ma che potesse simulare le attività del cervello umano, «manipolando simboli formali»²³.

In questo senso le osservazioni di Searle, secondo il quale il computer può benissimo superare la prova di Turing senza "comprendere nulla", possono essere condivise. Al fine di equiparare la macchina alla mente, infatti, non sarebbe sufficiente che la macchina potesse riprodurre gli stati cognitivi della mente, poiché ciò che caratterizza gli stati mentali della mente umana è l'intenzionalità, che dipende dai procedimenti causali e non da quelli formali:

Il problema, col simulatore del cervello, è che simula le cose sbagliate del cervello. Finché simula solo la struttura formale della sequenza delle aggregazioni di neuroni e della sinapsi, non avrà simulato ciò che importa nel cervello: precisamente le sue proprietà causali, la sua abilità a produrre stati intenzionali²⁴.

I sostenitori dell'IA forte, secondo John Searle, non si avvedono di riproporre nelle loro teorie un "dualismo mascherato"²⁵ in base al quale *res cogitans* e *res extensa*, di cartesiana memoria, sarebbero, seppure non empiricamente, almeno teoricamente separabili, in modo tale che sia possibile riprodurre il funzionamento della mente indipendentemente dal sostrato causale del cervello.

D'altro canto, secondo l'autore, gli stessi sostenitori dell'IA forte peccherebbero di un certo comportamentismo, e questo vizio di fondo indurrebbe gli stessi a ritenere di aver riprodotto e reso osservabile la causa degli stati cognitivi, che per l'uomo è nel cervello, per il solo fatto di aver riprodotto, mediante manipolazione di simboli formali, gli stati cognitivi o processi mentali nel calcolatore elettronico:

Poiché i computer, programmati appropriatamente, possono avere modelli input-output simili a quelli degli esseri umani, siamo tentati di postulare che essi abbiano stati mentali simili agli stati mentali umani. Ma una volta che vediamo che è possibile, sia concettualmente che empiricamente, che un sistema abbia capacità umane in qualche campo senza avere alcuna intenzionalità, dovremmo poter superare questo impulso²⁶.

Se si ripercorre il ragionamento dei comportamentisti in effetti si può riscontrare che il sillogismo è viziato, in quanto si fonda su una premessa che postula un'equivalenza inesistente: «la mente sta al cervello come il software sta

20. TURING 1950, pp. 148-149: «Il lettore si sarà già accorto che non ho alcuna argomentazione molto convincente di carattere positivo per sostenere il mio punto di vista. Se l'avessi avuta non mi sarei certo dedicato con tanta cura a indicare gli errori dei punti di vista opposti al mio».

21. SEARLE 1984, p. 55.

22. TURING 1950, pp. 121-122.

23. SEARLE 1984, p. 58.

24. *Ivi*, p. 60.

25. *Ivi*, p. 71.

26. *Ivi*, p. 69.

all'hardware e così possiamo capire la mente senza fare neurofisiologia»²⁷.

3. Neuroplasticità e *Intelligenza meccanica*

Ciò che si propone questo studio è mettere a disposizione di altre discipline, come il diritto o la bioetica, i risultati degli studi sul cervello, al fine di demistificare alcune proposizioni indimostrate e del tutto infondate.

In particolare, sembra che oggi sia dato per assiomatico l'assunto secondo il quale riprodurre in calcolatori elettronici alcune attività e procedure, alcune manifestazioni del cervello, implichi e giustifichi due ulteriori affermazioni: 1) che possiamo dire ormai che il cervello sia conoscibile, come si conosce un oggetto empirico; 2) che il cervello si riduca a quelle attività o funzioni.

Se tali affermazioni fossero vere, allora i discorsi di Searle sull'intenzionalità cadrebbero, in quanto nulla di differente e specifico avrebbero gli stati cognitivi umani rispetto agli stati cognitivi della macchina.

Al contrario, gli studi condotti negli ultimi decenni sul cervello che interagisce con le tecnologie digitali hanno evidenziato alcune caratteristiche peculiari del cervello, in particolare una, che è nota come neuroplasticità²⁸.

Questo significa che il nostro cervello non solo è in grado di apprendere ed elaborare informazioni, ma esso cambia continuamente a causa delle esperienze e acquisizioni, sia cognitive, sia neuro-sensoriali.

Lo stesso vissuto, i progetti, le percezioni e i comportamenti, ancor più se ripetuti, conformano e modellano i circuiti cerebrali.

Le macchine non hanno esperienze allo stesso modo in cui gli uomini le hanno, poiché gli uomini conoscono e sperimentano attraverso la corporeità che è parte integrante e inscindibile, dell'essere persona²⁹.

4. *Menti, cervelli ... e coscienze*

Se si prende sul serio la qualità neuroplastica³⁰ dei circuiti cerebrali, si comprende come anche la conoscenza non sia un'attività solo mentale³¹ ma risieda in molti luoghi corporei diversi, seppure a volte si localizzi in transito a partire da alcune terminazioni neuro-sensoriali (quando tocchiamo il fuoco e subiamo una bruciatura; quando vediamo un lampo o ascoltiamo un tuono, etc.).

Alcuni studi in psicologia hanno approfondito ciò che la disciplina chiama "schema corporeo"³² per sottolineare che l'attività conoscitiva non è solo intellettuale, ma passa per il nostro corpo e le nostre azioni. Queste ricerche hanno evidenziato che spesso non troviamo «dove finiamo noi e dove inizia il resto del mondo», ovvero la nostra coscienza, perché «l'abbiamo cercata nel posto sbagliato»³³.

I nostri corpi e le nostre menti sono attive. Cambiando la forma della nostra attività possiamo cambiare la nostra stessa forma, il nostro corpo e la nostra mente ... Oggi pensiamo all'economia come a qualcosa di globalizzato, alle società per azioni come a qualcosa di internazionalizzato e alle reti informatiche come qualcosa di diffuso. Noi stessi siamo per natura dinamicamente distribuiti, in grado di oltrepassare i confini e situati in un ambiente³⁴.

Riprendendo Searle, il fatto che possiamo riprodurre determinate operazioni mentali o stati

27. *Ivi*, p. 59.

28. PASCUAL LEONE-AMEDI-FREGNI-MERABET 2005.

29. SPAEMANN 2013; cfr. sul punto gli studi di antropologia biblica di FREVEL 2009, pp. 258-260: «... Il cuore può essere sinonimo di volontà, progetto, senso, sentimento. Oltre alle funzioni di tipo emotivo e volitivo, si legano al cuore pure quelle noetiche. L'uomo veterotestamentario non pensa con la testa ma con il cuore ... Il cuore è la sede dell'intelletto, della ragione, della coscienza, della facoltà cognitiva, della percezione, della memoria, della capacità di apprendere, riflettere e giudicare, della ponderazione argomentata».

30. Cfr. SONG-MILLIDGE-SALVATORI et al. 2024.

31. Cfr. GANDOLFINI 2013; nonché PALAZZANI-ZANNOTTI 2013.

32. Il riferimento è a NOË 2010, p. 81.

33. *Ivi*, p. 72.

34. *Ivi*, p. 71 ss.

cognitivi in un procedimento computazionale non significa che quel modello computazionale svolga quelle operazioni allo stesso modo del cervello umano³⁵.

Questo non solo è evidente a livello esperienziale³⁶, ma l'inferenza secondo la quale se un procedimento computazionale mi fornisce lo stesso risultato di un'operazione mentale, allora tutte le operazioni mentali non sono altro che procedimenti computazionali, è teoricamente errata, per diversi ordini di motivi.

In primo luogo, non tutte le operazioni mentali sono riproducibili da una macchina, ovvero non potrei trasferire la modalità umana di pensare nella macchina, ma solo far sì che questa simuli le sequenze logiche e i procedimenti causali onde ottenere lo stesso prodotto.

L'errato sillogismo, che è alla base del pensiero contestato da Searle, sarebbe formulabile all'incirca come segue:

premessa A – se un'attività è riproducibile da una macchina è (espressione della natura) meccanica,

+ premessa B – se gli stati mentali umani sono riproducibili da una macchina,

= conclusione – dunque il cervello è una macchina.

In realtà gli errori sono presenti in più di un passaggio: nell'articolo determinativo "gli" che induce a ritenere che "tutti" gli stati mentali siano riproducibili da una macchina, piuttosto che solo "alcuni"; nel salto logico che attribuisce al cervello una natura, sulla base di un tipo di attività che svolge. Il cervello può esprimersi in una molteplicità di attività diverse, delle quali solo una minima parte è formulabile in modelli computazionali; allo stesso modo se un animale, come un pappagallo o una scimmia, può riprodurre un comportamento

umano, non vuol dire che l'imitazione dell'azione implichi l'uguaglianza degli agenti.

In secondo luogo, il fatto che la macchina possa eseguire alcune attività umane, non solo logiche, ma anche pratiche, non è sufficiente ad inferire che la macchina possa essere equiparata all'uomo e, viceversa, l'uomo a una macchina.

5. Il riduzionismo scienziasta

La prospettiva meccanicista e scienziasta, sopra rappresentata, risulta infondata. Non soltanto l'attività cerebrale non è conoscibile come quella di un oggetto allo studio delle sole scienze empiriche, perché le nostre menti sono "estese"³⁷ e sono integrate nel nostro "schema corporeo". Ma neanche l'attività mentale stessa è riducibile a quella meccanica.

Dalle sopra esposte considerazioni emerge con vigore la questione antropologica nel rapporto tra tecnologie e essere umano: l'utilizzo e lo sviluppo dell'IA non costituisce tanto un problema bioetico in quanto strumento per molteplici attività, tra le quali le attività sanitarie, ma nella misura in cui pone le basi per un "cambiamento d'epoca"³⁸ dell'umano.

Secondo l'approccio scienziasta³⁹ posso conoscere solo ciò che posso osservare e misurare, di conseguenza la realtà, anche l'uomo, è ridotto a ciò che di lui posso osservare e misurare. La deriva di questa teoria consiste nel negare l'esistenza di tutto ciò che non è misurabile empiricamente, con presupposto ideologico e atteggiamento antiscientifico: ciò che non posso misurare, non esiste.

Il *bias* del riduzionismo scientifico consiste nel dedurre dallo studio del cervello e dalla riproducibilità di alcune operazioni logiche in calcolatori elettronici, che il cervello non sia altro che una macchina.

35. SEARLE 1984, p. 69: «Il fatto che il programmatore e l'interprete dell'output usano i simboli come sostituti di oggetti nel mondo è totalmente al di fuori degli obiettivi del computer. Il computer, per ripeterci, ha una sintassi ma non una semantica. ... Il punto non è che esso manca di qualche informazione di secondo ordine per l'interpretazione dei suoi simboli di primo ordine, ma piuttosto che i suoi simboli di primo ordine non hanno interpretazioni almeno per quanto riguarda il computer. Tutto ciò che il computer ha, sono simboli».

36. Cfr. GALLAGHER-ZAHAVI 2009.

37. Cfr. NOË 2010.

38. FRANCESCO 2022.

39. COWBURN 2013.

Il successivo passaggio riduzionista, indotto dalla *Cognitive Science*⁴⁰, sarebbe che il funzionamento del cervello esaurisce il pensiero e la riflessione prudenziale: anche questo risulta essere un assunto apodittico, poiché le scienze neurologiche e psicologiche dimostrano che l'uomo è molto più delle sue capacità cognitive e che il suo cervello produce un pensiero personale, che la macchina mai potrà riprodurre. Chiamiamo coscienza⁴¹ ciò che si sottrae alla misurazione e all'osservazione empirica.

L'errore delle scienze cognitive, evidenziato da Searle, è che esse intendono studiare il funzionamento della mente, sulla base del presupposto che il pensiero sia pur sempre un'attività astratta e separata rispetto al cervello, ovvero che «la mente sia un tipo di computer»⁴². Nonostante quelle teorie ritengano che «non sia sufficiente simulare le operazioni della mente per spiegare l'intelligenza umana»⁴³, alla fine riducono pur sempre il pensiero ad operazioni su codici simbolici.

Anche se le macchine diventassero capaci di apprendere e «staccarsi dal comportamento prevedibile implicato nel calcolo», ovvero diventassero intelligenti nel senso in cui lo intende Turing, ciò non cambierebbe il discorso di fondo, e cioè che è ingiustificato inferire dall'attività logico-meccanica che la causa di essa sia, o possa diventare, un'intelligenza del tipo di quella umana: rimarrà pur sempre un'intelligenza meccanica.

6. Un modello normativo per i sistemi di IA

Il possibile utilizzo dell'IA nell'ambito sanitario solleva alcuni quesiti giuridici ulteriori, rispetto a quelli che sorgono in qualsiasi altro settore, a causa delle specificità e complessità dell'atto medico, che può essere definito come condotta – guidata

da conoscenze tecnico-scientifiche “fisico-chimico-biologiche” e innestata su “dinamiche relazionali”⁴⁴ – finalizzata alla cura, alla promozione della vita e della salute o del completo benessere psico-fisico del paziente.

Assumendo la prospettiva sopra descritta, al fine di comprendere le ricadute giuridiche sulla relazione medico-paziente delle applicazioni di IA, è necessario chiedersi in quali fasi dell'attività di cura si collochino le operazioni degli agenti intelligenti artificiali e se questi siano autonomi centri di imputazione di atti *lato sensu* medici; se integrino una componente modale o strumentale – un ausilio – dell'atto imputabile al professionista; o ancora se possano essere ricondotti alla figura dell'ausiliario, a causa della parziale autonomia dei processi che da essi si originano.

L'impianto normativo dell'*AI Act*, Regolamento UE 2024/1689⁴⁵, non affronta questi quesiti in modo diretto, poiché non inquadra il sistema di IA dal punto di vista del diritto sostanziale, bensì ne regola l'utilizzo dal punto di vista procedurale.

Infatti, sebbene sia stata sostenuta l'ipotesi dell'attribuzione di una soggettività giuridica al sistema di IA, come persona giuridica dotata di un patrimonio o *e-person*, questa soluzione non è stata avallata né dalla dottrina prevalente né tantomeno dal legislatore europeo. L'analisi del giurista deve pertanto limitarsi a ricavare i collegamenti e comporre un quadro d'insieme tra la recentissima regolamentazione sull'IA e la disciplina vigente a livello euro-unitario e nazionale sulla responsabilità del produttore e sull'attività sanitaria. In questo modo l'adozione di una normativa sull'IA, che chiarisca obblighi e responsabilità dei diversi soggetti coinvolti, dovrebbe conseguire l'effetto di

40. LEPORE-PYLYSHYN 1999.

41. Cfr. BAYNE-CLEEREMANS-WILKEN 2009.

42. PYLYSHYN 1999, p. 12.

43. *Ibidem*, la traduzione è dell'autore.

44. BELLINO 2015.

45. Il testo del Regolamento (UE) 2024/1689 è stato approvato dal Parlamento europeo in data 13 marzo 2024 e dal Consiglio dell'Ue in data 21 maggio; è stato pubblicato nella *Gazzetta Ufficiale dell'Unione europea* in data 12 luglio 2024 e, alla data del 16 luglio 2024. Ormai esauriti i passaggi dell'iter procedurale, sarà applicabile dal 2 agosto 2026, ma l'art. 6 comma 1 a partire dal 2 agosto 2027, cfr. Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

ingenerare sicurezza e fiducia negli utilizzatori e, allo stesso tempo, incentivare il progresso tecnologico e lo sviluppo del mercato.

Dal punto di vista giuridico è necessario comprendere in che modo e misura i movimenti dei robot o gli output di un software possano concorrere ad integrare la condotta del professionista o operatore sanitario: se costituiscano un *medium* – un'estensione del medico o un suo potenziamento – oppure a pieno titolo un agente al pari di un ausiliario, al fine di poter rispondere alle domande sopra esposte.

L'AI Act enuncia esplicitamente le finalità della regolamentazione adottata, ovvero quelle di «migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile»⁴⁶ garantendo la tutela dei diritti fondamentali, dello Stato di diritto, della democrazia in conformità ai valori dell'Unione.

L'attenzione specifica di giuristi e legislatori è stata richiamata durante gli ultimi decenni, nei quali si sono sviluppate queste sofisticate tecnologie, dal fatto che esse possono incorporare meccanismi decisionali automatizzati, che mettono a

rischio interessi e beni giuridici primari, protetti dagli ordinamenti nazionali e internazionali: la vita e la salute umana; la sicurezza di tutti gli operatori sanitari, del paziente e dell'umanità intera; la deontologia della professione medico-sanitaria; l'innovazione tecnologica e gli investimenti industriali; gli interessi di mercato.

Per comporre queste posizioni giuridiche, diritti e interessi, in un delicato equilibrio, sono stati necessari diversi anni, durante i quali si sono svolti i lavori preparatori⁴⁷ e sono stati interpellati organi consultivi⁴⁸ e gruppi di esperti⁴⁹, al fine di pervenire alla stesura di una prima proposta nel 2021⁵⁰ ed alla redazione dell'articolato attuale.

Già il testo del 2021 – che è stato in gran parte confermato dal provvedimento di recente approvato, seppur con alcuni emendamenti di rilievo – presceglieva l'impianto normativo dei sistemi di gestione dei rischi o *New Legislative Framework*⁵¹.

Questo tipo di struttura regolatoria richiede a coloro che intraprendono un'attività connotata da rischi di vario genere, ineliminabili in radice, di costruire un modello di organizzazione e stabilire determinate procedure che, pur contemplando l'ipotesi di verifica del rischio⁵², cercano di

46. [Art. 1, comma 1.](#)

47. Si fa riferimento in ambito Ue alle Comunicazioni e proposte succedutesi negli ultimi dieci anni, tra le quali principalmente: Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Piano coordinato sull'intelligenza artificiale*, 7 dicembre 2018, [COM\(2018\) 795](#); Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Creare fiducia nell'intelligenza artificiale antropocentrica*, 8 aprile 2019, [COM\(2019\) 168](#); Commissione europea, *Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia*, 19 febbraio 2020, [COM\(2020\) 65](#).

48. EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES 2018.

49. HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE 2019, 2019-A, 2020. Si veda anche lo studio JOINT RESEARCH CENTRE 2020.

50. Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, 21 aprile 2021, [COM\(2021\) 206](#).

51. Lo schema normativo del *New Legislative Framework* è descritto in dettaglio nel Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio del 9 luglio 2008 che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93.

52. Nei sistemi di gestione dei rischi gli eventi che integrano la "non conformità" o discostamento dallo standard, sono i più vari, a seconda del campo al quale si applica l'apparato di prevenzione, ad es.: nel campo industriale, malfunzionamento o errato funzionamento di macchinario con esito dannoso nei confronti di cose o persone; in attività commerciali, l'illecito commesso da un dipendente d'azienda; nelle aziende di tutti i tipi, l'infortunio del lavoratore; negli istituti di formazione e istruzione, la lesione, volontaria o involontaria, dello studente nei locali o pertinenze della scuola, ecc.

limitarne la probabilità di ricorrenza e ridurne al minimo l'impatto.

L'assunzione di una percentuale di alea – di scostamento dallo standard o esito atteso –, come *condicio sine qua non* dell'esercizio dell'attività *de qua*, comporta un ribaltamento di prospettiva da parte del legislatore: la disciplina non può, a meno di vietare del tutto la prassi, descrivere astrattamente la verifica del rischio come ipotesi "patologica" di per sé indicativa di una colpa, bensì può assumere come presupposto che, chiunque "agisca" o "subisca" l'attività pericolosa, abbia accettato quel rischio e le connesse conseguenze giuridiche in termini di imputazione e regime di responsabilità.

La normativa pertanto stabilisce modelli procedurali e requisiti formali ai quali i produttori – ma anche nelle altre fasi i fornitori⁵³, assembleatori, gestori, sviluppatori e utilizzatori – devono attenersi, per ottenere la conseguente valutazione di conformità del sistema di IA e l'autorizzazione all'immissione in circolazione.

Similmente alla circolazione dei veicoli a motore, per i quali è previsto l'obbligo assicurativo⁵⁴ a carico del proprietario, così anche per le attività, che si servono di sistemi di IA, l'autorizzazione all'immissione in circolazione del robot o software non garantisce l'assenza di rischio, bensì assolve a una precisa *ratio legis*, quella di prevedere ed attuare un complesso di misure per tenere l'alea sotto controllo e ridurla al minimo.

Dall'esame degli articoli da 8 a 15 e da 16 a 27⁵⁵, si evince la struttura del modello, ovvero una serie di controlli preventivi, precauzioni e sanzioni, oltre che l'assoggettamento ad una sorveglianza continua. All'articolo 9 rubricato "Sistemi di gestione dei rischi", precisamente al comma 2 sono descritte in sequenza le quattro operazioni principali in cui si sostanzia la disciplina: identificazione e analisi

dei rischi; valutazione della loro probabilità di evenienza; monitoraggio successivo e verifiche periodiche; trattamento dei rischi al fine dell'obiettivo del miglioramento continuo.

Quello descritto è, in forma molto semplificata, lo schema normativo dei sistemi di gestione dei rischi delle organizzazioni (aziendali), paradigma che si sta affermando in molteplici settori non solo industriali, tramite normative cosiddette "tecniche" (peraltro anche in settori nient'affatto tecnici).

7. L'attività dei sistemi di IA sotto la lente del diritto: definizioni e classificazioni

La definizione di sistema di IA contenuta all'articolo 3, n. 1 deve ormai essere considerata normativa: questo è «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali».

La grande partizione introdotta dalla normativa è data dalla distinzione tra le diverse tipologie di rischio indotto dai sistemi di IA: alcuni di essi realizzano attività vietate, descritte all'articolo 5, perché implicano un livello o qualità di rischio inaccettabile; altre pratiche, di cui agli articoli 6-7, sono ritenute a rischio accettabile ma elevato, per l'effetto i sistemi che le dispiegano sono definiti "ad alto rischio" e assoggettati a verifiche e requisiti rigorosi; tutti gli altri sono definiti in via residuale a rischio basso o minimo.

Il divieto⁵⁶ di produzione e di utilizzo, previsto dall'articolo 5, vige per quei sistemi di IA considerati, di per sé o per l'uso che se ne può fare, particolarmente pericolosi, come chiarisce il

53. Cfr. D'ADDA 2022.

54. Cfr. la Risoluzione del Parlamento europeo del 2017 sulla robotica, che ipotizza al n. 58 l'applicazione ai robot del regime di assicurazione obbligatoria vigente per i veicoli a motore: «ritiene che, come avviene nel caso dell'assicurazione dei veicoli a motore, tale regime assicurativo potrebbe essere integrato da un fondo per garantire la possibilità di risarcire i danni in caso di assenza di copertura assicurativa», Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)).

55. Rispettivamente Sezioni 2 e 3 del Capo III.

56. Art. 5 "Pratiche di IA vietate" in particolare riferimento ai sistemi di IA che attribuiscono un punteggio sociale in base ai comportamenti individuali, cfr. CERRINA FERONI 2023.

Considerando 28⁵⁷, in riferimento a quei sistemi per i quali il rischio per la salute, la sicurezza e i diritti fondamentali è considerato inaccettabile.

In questa sede sembra rilevante menzionare tra i sistemi vietati quelli manipolatori (lett. a) del comma 1 – in grado di influire sulla volontà e le scelte dei singoli – e classificatori (lett. c) del comma 1 delle persone, in grado di ingenerare effetti distorsivi a livello sociale, poiché regolano, ad esempio, con criteri discriminatori l’accesso o la distribuzione di beni e di servizi, in special modo se adottati da pubbliche amministrazioni per la gestione di servizi pubblici essenziali. Oltre a ciò, sono inclusi nell’elenco dei sistemi vietati quelli che consentono «l’identificazione biometrica “in tempo reale” in spazi accessibili al pubblico» (lett. h), comma 1 senza alcuna informazione a coloro che vi sono coinvolti e senza che sussista una delle situazioni previste a giustificazione di eccezioni al divieto.

L’articolo 6 invece qualifica come ad alto rischio il sistema che «presenti un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel senso di influenzare materialmente il risultato del processo decisionale»⁵⁸.

Per i sistemi di IA ad alto rischio il Regolamento prevede determinati requisiti – rispetto ai quali i produttori, fornitori e utilizzatori devono essere *compliant*, come l’adozione di un sistema di gestione dei rischi (cfr. art. 9) – affinché possano essere immessi sul mercato o in servizio⁵⁹.

Nonostante il comma 1 dell’articolo 6 statuisca la regola generale che assoggetta i sistemi “ad alto rischio” ad una serie rigorosa di controlli, monitoraggio e verifiche ed il comma 2 qualifichi di default “ad alto rischio” tutti i sistemi appartenenti ad uno dei settori di cui all’allegato III⁶⁰, tuttavia il comma terzo dello stesso articolo introduce una deroga di non poco conto. Tale norma stabilisce che alcuni sistemi, pur da considerare “ad alto rischio” perché rientranti in una delle categorie di cui all’elenco dell’allegato III – tra i quali, ciò che qui interessa, i dispositivi medici – sono eccezionalmente esclusi dalla qualificazione e sottratti alla relativa disciplina, qualora sussista una delle condizioni espressamente specificate dalle lettere da a) a d).

Trattandosi di norma speciale che deroga a quella generale, la lettura del testo, integrata dal superiore comma 2, produce la seguente affermazione: alcuni sistemi di IA, che dovrebbero essere considerati ad alto rischio, perché incidenti su diritti fondamentali o interessi di rilievo pubblico, non sono considerati tali, purché sussista una o più delle seguenti condizioni: «a) il sistema di IA è destinato a eseguire un compito procedurale limitato; b) [...] a migliorare il risultato di un’attività umana precedentemente completata; c) [...] a rilevare schemi decisionali o deviazioni da schemi decisionali precedenti e non è finalizzato a sostituire o influenzare la valutazione umana [...]; d) [...] a eseguire un compito preparatorio per una valutazione pertinente ai fini dei casi d’uso elencati nell’allegato III»⁶¹.

57. Considerando 28: «L’IA presenta, accanto a molti utilizzi benefici, la possibilità di essere utilizzata impropriamente e di fornire strumenti nuovi e potenti per pratiche di manipolazione, sfruttamento e controllo sociale. Tali pratiche sono particolarmente dannose e abusive e dovrebbero essere vietate poiché sono contrarie ai valori dell’Unione relativi al rispetto della dignità umana, alla libertà, all’uguaglianza, alla democrazia e allo Stato di diritto e ai diritti fondamentali sanciti dalla Carta, compresi il diritto alla non discriminazione, alla protezione dei dati e alla vita privata e i diritti dei minori».

58. Art. 6. *Regole di classificazione per i sistemi di IA ad alto rischio*.

59. Per la differenza tra “immissione sul mercato”, “messa a disposizione sul mercato” e “messa in servizio” confronta art. 3 “Definizioni”, rispettivamente nn. 9, 10 e 11.

60. Si ricordano in breve le otto categorie ad alto rischio ex Allegato III: «Biometria..., Infrastrutture critiche..., Istruzione e formazione professionale..., Occupazione, gestione dei lavoratori e accesso al lavoro autonomo..., Accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali..., Attività di contrasto..., Migrazione, asilo e gestione del controllo delle frontiere..., Amministrazione della giustizia e processi democratici ...».

61. Art. 6, comma 3 che riprende il Considerando 53.

Questa norma solleva rilievi critici sia quanto alla formulazione, alquanto tortuosa, sia quanto al contenuto, poiché le deroghe introdotte aprono all'interpretazione spazi troppo ampi. Non è chiaro cosa voglia dire che un sistema di IA, seppure appartenente ad una delle categorie di cui all'allegato III, non sia da considerare ad alto rischio, perché debba «eseguire un compito procedurale limitato»⁶² e chi decida su questa qualificazione. La stessa osservazione vale per gli altri tre casi di deroga, da b) a d), poiché queste disposizioni implicano valutazioni ampiamente discrezionali attribuendo un minor livello di pericolosità a sistemi che incidono, *ab origine* a causa del settore in cui operano, su diritti fondamentali, sulla salute o sulla sicurezza dei cittadini.

8. Responsabilità per l'utilizzo dei sistemi di IA in ambito sanitario

Sebbene appaiano di grande portata i possibili benefici dei sistemi di IA applicati al procedimento clinico, in termini di velocità della diagnosi, personalizzazione e precisione delle terapie, nondimeno un malfunzionamento o errore, c.d. *bias*, del sistema può determinare conseguenze anche gravi, o letali, a danno della salute o dell'integrità fisica delle persone.

La questione del danno prodotto da sistema di IA per produzione di output errato o mancata produzione dell'output, riguarda il tema della responsabilità.

8.1. L'imputazione soggettiva: le figure coinvolte nella catena di valore dell'IA

Il legislatore europeo mediante l'adozione del *NLF* affronta le fondamentali questioni giuridiche insorte a seguito dello sviluppo delle applicazioni di IA – principalmente quelle dell'imputazione delle attività nelle diverse fasi, dalla programmazione alla messa in servizio, e delle conseguenti responsabilità – in modo indiretto, disponendo a carico di coloro, che entrano nella catena del valore dell'IA⁶³ – soprattutto per i sistemi ad alto rischio – obblighi e adempimenti, a seconda del ruolo che assumono nell'assemblaggio del prodotto “finito”.

Già è stato accennato che il modello del sistema di gestione dei rischi – applicato a molteplici enti quali aziende, industrie, società commerciali e finanziarie, operanti in diversi settori – in ossequio alla logica dei sistemi di gestione, non ha lo scopo di stabilire con precisione il limite tra il lecito e l'illecito, ma di imporre all'organizzazione (aziendale, ecc.) di collocare ogni sequenza della propria attività in una complessa procedura e di mantenerla sotto un costante monitoraggio, allo scopo di rilevare in quale sezione si verifichi eventualmente la difformità o scostamento dallo standard, al fine di adottare misure correttive e realizzare il miglioramento continuo.

Nei diversi comparti di attività d'impresa una certa tipologia o percentuale di rischi – fotografati all'inizio della costruzione del “modello” organizzativo nel documento chiamato “analisi dei rischi” o *risk assessment* – è insita e prevedibile fin dall'origine. La cosiddetta “non conformità” o allontanamento dall'iter procedurale atteso rappresenta una fattispecie astratta che di volta in volta può essere integrata da atti o fatti molto diversi tra loro: azioni od omissioni di ausiliari (compresa la commissione di reati); malfunzionamenti di attrezzature o impianti, oppure errori di utilizzo, che provocano danni a terzi.

Trasferendo questa logica alla produzione dei sistemi di IA, considerata la difficoltà di ipotizzare preventivamente tutte le diverse correlazioni⁶⁴ e implicazioni tra soggetti che compartecipano alla fabbricazione di un sistema siffatto, è comprensibile che il Regolamento non affronti in modo diretto il principale problema in punto di diritto, che è quello dell'imputazione e conseguente responsabilità dei danni provocati dai sistemi di IA, ma rinvii in forma implicita alla normativa europea e nazionale in merito, ovvero attenda che la Commissione si esprima con un proprio orientamento.

Lo schema normativo dell'*AI Act* fornisce purtuttavia il quadro dei soggetti obbligati ad adottare misure preventive e correttive dei rischi, di talché la mancata osservanza delle formalità, comporta per ciò stesso un comportamento colpevole ed un correlato addebito.

62. Art. 6 comma 3.

63. Questa espressione compare nel testo del Regolamento per la prima volta al Considerando 9.

64. Per un'analisi approfondita delle figure che partecipano alla produzione dei sistemi di IA e dei criteri di imputazione delle responsabilità in caso di verifica di danni v. D'ADDA 2022.

Ad un primo esame del testo si può notare come l'attenzione del legislatore sia sbilanciata verso le figure che intervengono nella parte finale della sequenza, nella fase della produzione e immissione in circolazione del prodotto: ben si comprendono le motivazioni che hanno indotto ad assumere tale prospettiva, ovvero quelle di favorire negli utilizzatori un convincimento sull'affidabilità di questi sistemi e di promuoverne la circolazione sul mercato, rendendo agevole per l'utente l'azionabilità di un'eventuale domanda di ristoro del danno.

Sebbene questa impostazione fosse stata suggerita già da una proposta di Regolamento sulla responsabilità per funzionamento dei sistemi di IA del 2020⁶⁵, tuttavia essa non ha avuto seguito, perché effettivamente troppo gravosa e penalizzante per gli operatori finali. Si pensi alle ricadute sulla relazione di cura di una siffatta scelta legislativa. Ciò provocherebbe in materia di responsabilità risarcitoria in ambito sanitario una legittimazione processuale passiva generalizzata delle strutture sanitarie e dei medici (salvo azione di rivalsa), con conseguente incentivo ad un'attitudine "difensiva" dei professionisti e generazione di una diffusa sfiducia nella categoria.

Da un'analisi accurata emerge invece che altri soggetti possono fornire un apporto, anche

rilevante, nella messa a punto di una componente del sistema, se non dell'intero prodotto: si tratta degli ideatori dell'algoritmo, programmatori, operatori di *front-end* o di *back-end*⁶⁶, assemblatore finale (che può essere produttore del robot e coincidere con il *deployer* o meno), fornitori⁶⁷, *deployer*⁶⁸, importatori⁶⁹, distributori⁷⁰ e gli utilizzatori finali.

Per i robot autonomi di intelligenza artificiale emerge il fondamentale apporto di chi partecipa alla ideazione del software, «procede con la codificazione – intesa come sviluppo dell'algoritmo così ideato in un codice interpretabile dalla macchina – ed infine involge un'attività di collaudo/testing»⁷¹. La medesima impresa che realizza il software potrebbe poi installarlo su un hardware, oppure immetterlo sul mercato, affinché possa essere sviluppato da un altro produttore di robot oppure dallo stesso utilizzatore finale.

Sul fornitore di un sistema ad alto rischio grava l'obbligo di adozione di un sistema di gestione dei rischi, con tutti gli adempimenti⁷² connessi, descritti negli articoli 9 e seguenti, come l'obbligo di trasparenza (v. *infra*), affinché siano conoscibili e conosciute dagli utenti le informazioni sulle caratteristiche tecniche dei prodotti e sui rischi potenziali (art. 11).

65. Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)).

66. Cfr. D'ADDA 2022, p. 816: «operatore, inteso come il soggetto che esercita un certo grado di controllo sul sistema di IA e che beneficia del suo funzionamento (si tratta dell'operatore di *front-end*) ovvero il soggetto che definisce le caratteristiche della tecnologia e fornisce i dati od il servizio di supporto al robot (l'operatore di *back-end*)».

67. Sui fornitori cfr. Considerando 79: «È opportuno che una specifica persona fisica o giuridica, definita come il fornitore, si assuma la responsabilità dell'immissione sul mercato o della messa in servizio di un sistema di IA ad alto rischio, a prescindere dal fatto che tale persona fisica o giuridica sia la persona che ha progettato o sviluppato il sistema».

68. Art. 3 n. 4

69. Sugli obblighi degli importatori, cfr. artt. 2, 20 e 23 e il Considerando 83.

70. Art. 24.

71. D'ADDA 2022, p. 826.

72. I sistemi ad alto rischio devono corrispondere ai requisiti di accuratezza, robustezza e cibersecurity, come già indicato dal Considerando 74: «Le prestazioni dei sistemi di IA ad alto rischio dovrebbero essere coerenti durante tutto il loro ciclo di vita e tali sistemi dovrebbero garantire un livello adeguato di accuratezza, robustezza e cibersecurity, alla luce della loro finalità prevista e conformemente allo stato dell'arte generalmente riconosciuto. La Commissione e le organizzazioni e i portatori di interessi pertinenti sono incoraggiati a tenere in debita considerazione l'attenuazione dei rischi e degli impatti negativi del sistema di IA. Il livello atteso delle metriche di prestazione dovrebbe essere dichiarato nelle istruzioni per l'uso che accompagnano il sistema».

Lo stesso fornitore potrebbe aver internalizzato⁷³ tutte le varie fasi della produzione, ma anche aver solo assemblato il sistema alla fine: la differenziazione per parcellizzazione o accentramento dei processi determina una difficoltà, da risolvere caso per caso, nella imputazione soggettiva dell'attività dell'IA, di particolare rilievo se lesiva di diritti altrui.

Di particolare importanza la figura, introdotta da ultimo nel testo, del *deployer* che

... dovrebbe essere interpretata come qualsiasi persona fisica o giuridica, compresi un'autorità pubblica, un'agenzia o altro organismo, che utilizza un sistema di IA sotto la sua autorità, salvo nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale. A seconda del tipo di sistema di IA, l'uso del sistema può interessare persone diverse dal *deployer*⁷⁴...

Nonostante alcune precisazioni definitorie sulle diverse figure operanti nella "catena del valore dell'IA", la legislazione di recente approvata prende in considerazione la difficoltà di individuare ruoli e responsabilità poiché

in determinate situazioni tali operatori [nda: gli importatori] potrebbero agire contemporaneamente in più di un ruolo e dovrebbero pertanto adempiere cumulativamente tutti gli obblighi pertinenti associati a tali ruoli. Ad esempio, un operatore potrebbe agire contemporaneamente come distributore e importatore⁷⁵.

Dalla complessità del quadro disegnato, emerge che un malfunzionamento di un sistema di IA potrebbe derivare dall'erroneo utilizzo dell'operatore finale, ma anche da un errore nella programmazione oppure nell'assemblaggio.

8.2. La ricostruzione oggettiva: tra obblighi di trasparenza e *explainability*

Un'altra criticità dei sistemi di IA, in particolare di quella generativa, è la cosiddetta "opacità intrinseca"⁷⁶ ovvero l'estrema difficoltà, per non dire l'impossibilità, di ricostruire *ex post* il processo svolto dall'agente intelligente per produrre l'output a partire dai dati in ingresso. Questa caratteristica rende ulteriormente difficoltosa la ricognizione oggettiva delle sequenze procedurali seguite dal sistema e della causa di un eventuale malfunzionamento.

Dal punto di vista tecnico questo problema era stato individuato fin dall'inizio dallo stesso Turing il quale nel suo celeberrimo saggio del 1950 doveva ammettere che la sfida, di cui all'epoca non si poteva intravedere la soluzione, era quella di educare o addestrare un calcolatore digitale allo stadio di "macchina-bambino" attraverso una tavola di istruzioni, ricompense e sanzioni, in modo da fornirgli non solo le regole per eseguire le operazioni da svolgere ma la propensione ad apprendere e formulare nuove regole⁷⁷. Questo processo di addestramento avrebbe dovuto in ogni caso rendere possibile ad ogni stadio intermedio di avere «una chiara immagine mentale dello stato della macchina in ogni momento del calcolo»⁷⁸. Nonostante la teoria fosse chiara, Turing doveva osservare che «una caratteristica importante di una macchina che impara è che il suo insegnante ignorerà spesso in gran parte ciò che di preciso si verifica al suo interno, quantunque possa essere in grado di predire in qualche misura il comportamento del suo allievo»⁷⁹.

La strategia di contrasto all'opacità, ampiamente discussa in fase di lavori preparatori dagli organi legislativi europei nelle diverse stesure, è stata tradotta a livello normativo nella formula

73. Questo è il fenomeno dei c.d. "sistemi chiusi", ovvero imprese nelle quali viene ideato, progettato, programmato e assemblato il prodotto completo, cfr. D'ADDA 2022, pp. 826-827.

74. Considerando 13.

75. Considerando 83.

76. Cfr. MESSINA 2023, la quale distingue tra opacità tecnica, giuridica e intrinseca, essendo quest'ultima: «un fenomeno che si manifesta allorché è la macchina a dettare autonomamente la regola, rendendo di fatto inaccessibile, anche agli stessi programmatori, l'iter che conduce all'esito dell'elaborazione delle informazioni», pp. 279-280.

77. TURING 1950, p. 148 ss.

78. *Ivi*, p. 155.

79. *Ibidem*.

dell'obbligo di trasparenza, gravante sui produttori e programmatori a tutela dei diritti degli utilizzatori e dei terzi, nei limiti strettamente necessari per non scoraggiare dall'altro lato l'innovazione tecnologica e l'invenzione industriale, protette da diritti di privativa.

Già la proposta del 2021 prevedeva all'art. 52 obblighi di trasparenza per tutti i sistemi di IA, non solo quelli ad alto rischio. La normativa da ultimo approvata richiama fin dalle prime battute questo requisito, che già l'*High-Level Expert Group on Artificial Intelligence* nelle sue *Ethics guidelines for trustworthy AI*⁸⁰ aveva enunciato come uno dei sette principi cardine della regolamentazione sull'IA: «intervento e sorveglianza umani, robustezza tecnica e sicurezza, vita privata e governance dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale e responsabilità». L'attuale Considerando 27, rinviando al *Parere del Gruppo di Esperti*, definisce la trasparenza come il fatto

che i sistemi di IA sono sviluppati e utilizzati in modo da consentire un'adeguata tracciabilità e spiegabilità, rendendo gli esseri umani consapevoli del fatto di comunicare o interagire con un sistema di IA e informando debitamente i *deployer* delle capacità e dei limiti del sistema e le persone interessate dei loro diritti⁸¹

Il legislatore europeo affronta chiaramente le "preoccupazioni relative all'opacità", prima che nell'articolato in senso stretto, nel Considerando 72⁸² ed insiste sulla spiegabilità dei sistemi di IA e sugli obblighi informativi che gravano sui programmatori e sui fornitori a monte dell'immissione in circolazione. Al fine di realizzare l'obiettivo della trasparenza, i sistemi di IA ad alto rischio

dovrebbero essere progettati in modo da consentire ai *deployer* di comprendere il funzionamento del sistema ... e ... essere accompagnati da informazioni adeguate sotto forma di istruzioni per l'uso.

Non solo è previsto l'obbligo di corredare il sistema di istruzioni per l'uso, ma sono altresì imposte

misure di sorveglianza umana, comprese le misure volte a facilitare l'interpretazione degli output del sistema di IA da parte dei *deployer*.⁸³

L'obbligo teorico si concretizza dunque in una serie di adempimenti menzionati all'articolo 1, e descritti in dettaglio negli articoli 13 e 50 (oltre che richiamati in modo sparso in altri luoghi del testo). Si ricorda che, mentre l'articolo 13 si riferisce solo ai sistemi di IA ad alto rischio, l'art. 50 si riferisce in generale a "determinati sistemi di IA", espressione che indica anche altri sistemi, a rischio basso o minimo.

L'articolo 13 rubricato "Trasparenza e fornitura di informazioni ai *deployer*", che nell'ultima formulazione sostituisce agli utenti i *deployer*, specifica il contenuto obbligatorio delle istruzioni per l'uso, richiedendo espressamente ai fornitori di includere nel documento alcuni elementi che consentano la spiegabilità e l'interpretabilità dell'output. In questo senso si sottolineano alcuni interventi innovativi rispetto alla proposta di Regolamento del 2021, quali le lettere b) iv) e vii) dell'art. 13, comma 3 nonché la lettera f):

Art. 13. ... 3. Le istruzioni per l'uso contengono almeno le seguenti informazioni: b) le caratteristiche, capacità e i limiti delle prestazioni del sistema di IA ad alto rischio, tra cui: ... iv) se del caso, la capacità e caratteristiche tecniche del

80. Cfr. HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE 2019. Ai sette principi guida per un'IA affidabile fa espresso riferimento il Considerando 27: «Sebbene l'approccio basato sul rischio costituisca la base per un insieme proporzionato ed efficace di regole vincolanti, è importante ricordare gli orientamenti etici per un'IA affidabile del 2019 elaborati dall'AI HLEG indipendente nominato dalla Commissione. In tali orientamenti l'AI HLEG ha elaborato sette principi etici non vincolanti per l'IA che sono intesi a contribuire a garantire che l'IA sia affidabile ed eticamente valida. I sette principi comprendono: intervento e sorveglianza umani, robustezza tecnica e sicurezza, vita privata e governance dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale e responsabilità. [...] Secondo gli orientamenti dell'AI HLEG con "intervento e sorveglianza umani" si intende che i sistemi di IA sono sviluppati e utilizzati come strumenti al servizio delle persone, nel rispetto della dignità umana e dell'autonomia» [il corsivo è redazionale].

81. Considerando 27.

82. Nel testo della proposta del 2021 corrisponde al n. 47, seppur con significative modifiche.

83. Considerando 72.

sistema di IA ad alto rischio connesse alla fornitura di informazioni pertinenti per spiegarne l'output; ...vii) se del caso, informazioni che consentano ai *deployer* di interpretare l'output del sistema di IA ad alto rischio e di usarlo in modo opportuno; ... f) se del caso, una descrizione dei meccanismi inclusi nel sistema di IA ad alto rischio che consente ai *deployer* di raccogliere, conservare e interpretare correttamente i log in conformità dell'articolo 12⁸⁴

Poiché si tratta di requisiti della fase di programmazione, l'obbligo riguarda i fornitori⁸⁵, come chiarito dall'art. 8, comma 2, anch'esso introdotto *ex novo* nell'ultima stesura. Nelle istruzioni per l'uso devono essere presenti una serie di altri elementi⁸⁶, tra i quali di particolare interesse le misure di sorveglianza umana, di cui al successivo articolo 14, previste alla lettera d), che richiama di nuovo la necessaria interpretabilità dell'output: «comprese le misure tecniche poste in essere per facilitare l'interpretazione degli output dei sistemi di IA ad alto rischio da parte dei *deployer*».

L'articolo 50 invece è rivolto a fornitori e *deployer* di «determinati sistemi di IA», che sono indicati nei successivi paragrafi da 1 a 4, ad esempio quelli «destinati a interagire *direttamente* con le persone fisiche» oppure sistemi di IA, «compresi i sistemi di IA per finalità generali, che generano contenuti audio, immagine, video o testuali sintetici», ed altri.

Poiché non è possibile in questa sede un approfondimento sulla categoria dei «modelli di IA per finalità generali»⁸⁷, si sottolinea che essa è stata introdotta dagli emendamenti del giugno 2023, mentre non era presente nella proposta del 2021.

In conclusione, stante l'impossibilità di stabilire *a priori* e in astratto criteri di attribuzione della responsabilità per danni, si dovrà risalire nel caso concreto allo stadio della procedura nel quale si è verificata la difformità e alla figura di volta in volta imputabile soggettivamente.

Considerata da un lato la difficoltà dell'individuazione dei *tortfeasors*, soggetti obbligati ad ottemperare nelle diverse fasi a prescrizioni e adempimenti; dall'altro la caratteristica opacità che rende difficile dal punto di vista oggettivo la ricostruzione dei processi, un regime di responsabilità per danni che facesse ricadere sul danneggiato l'onere di provare la colpa del soggetto imputabile del malfunzionamento (che potrebbe derivare persino dallo stadio della programmazione) – a meno che non sia derivato da macroscopica imperizia dell'utilizzatore finale – e il nesso di causalità tra condotta colpevole e danno, risulterebbe oltremodo gravoso.

Nella disamina⁸⁸ dei diversi regimi di responsabilità applicabili, ad esempio, nell'ordinamento civilistico italiano, si potrebbe discutere dei *pro* e *contra* relativi all'adozione del regime di responsabilità extracontrattuale oppure di un'imputazione

84. Dal testo del Regolamento 2024/1689.

85. Nel Considerando 84 è chiarito che «Al fine di garantire la certezza del diritto, è necessario chiarire che, a determinate condizioni specifiche, qualsiasi distributore, importatore, *deployer* o altro terzo dovrebbe essere considerato un fornitore di un sistema di IA ad alto rischio e, pertanto, assumere tutti gli obblighi del caso», e cfr. Considerando 79.

86. Art. 13, comma 3 lettere da a) a f): «a) l'identità e i dati di contatto del fornitore e, ove applicabile, del suo rappresentante autorizzato; ... c) eventuali modifiche apportate al sistema di IA ad alto rischio e alle sue prestazioni che sono state predeterminate dal fornitore al momento della valutazione iniziale della conformità ...; e) le risorse computazionali e di hardware necessarie, la durata prevista del sistema di IA ad alto rischio e tutte le misure di manutenzione e cura, compresa la relativa frequenza [omissis]; f) se del caso, una descrizione dei meccanismi inclusi nel sistema di IA ad alto rischio [omissis]».

87. Nel testo definiti dall'art. 3, n. 63: «un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato da una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato».

88. Cfr. COLLETTI 2021; D'ADDA 2022, p. 830 ss.

a titolo di responsabilità oggettiva per i danni derivanti da sistemi di IA.

La scelta del regime di responsabilità extracontrattuale è stata caldeggiata da una proposta di direttiva⁸⁹ sulla responsabilità civile extracontrattuale da attività dei sistemi di IA, pur con il correttivo di una presunzione circa il nesso di causalità tra difetto e danno, per non gravare il danneggiato di un onere della prova troppo difficoltoso. L'elezione di una disciplina della responsabilità a titolo di *strict liability* sarebbe invece sostenuta dall'inquadramento dell'attività dei sistemi di IA tra le attività pericolose *ex art. 2050 c.c.* oppure nella fattispecie della responsabilità per danno cagionato da cose in custodia *ex art. 2051 c.c.*, o ancora della responsabilità per atti commessi da dipendenti e ausiliari *ex art. 2049 c.c.* Qualora fosse riconosciuto il sistema di IA come prodotto, sarebbe inoltre possibile l'iscrizione della responsabilità al produttore per danno da prodotto difettoso sia ai sensi della normativa nazionale, di cui al Codice del consumo⁹⁰, sia ai sensi della normativa europea⁹¹ stabilita dalla Direttiva 85/374/CEE, della quale è in discussione una proposta di revisione⁹².

Un'attenta ponderazione dovrebbe condurre a prescegliere un regime di responsabilità agevole per il danneggiato il quale potrebbe agire nei confronti dell'ultimo utilizzatore, di modo che non sia scoraggiato l'utilizzo di questi sistemi, salvo poi la proponibilità dell'azione di regresso del *solvens* nei confronti "del" o "dei" coobbligati, secondo criteri di riparto della responsabilità che tengano conto dei diversi regimi (in deroga all'art. 2055 c.c.), sulla base dei quali rispondono i (plurimi) condebitori, a titolo di colpa o a titolo oggettivo, per non gravare

dall'altro lato l'utilizzatore dell'intera responsabilità per il semplice fatto di aver introdotto il rischio.

Inoltre per calibrare in modo equo la responsabilità di ciascuno dei soggetti che hanno contribuito alla catena produttiva sarà necessario «accertare il ruolo delle attività riconducibili a tali soggetti nella causazione del sinistro»; pertanto la quota di ciascuno nell'obbligazione risarcitoria «si fonderà sul grado della colpa associabile alle diverse condotte, sull'intensità dell'apporto causale dispiegato da ciascuno, e sulla dimensione del rischio riconducibile ad ogni *tortfeasor*»⁹³.

Nel caso di sistemi utilizzabili in ambito sanitario la gravità del rischio è data dall'importanza dei beni in gioco ovvero la vita e la salute: questo giustifica il superamento del criterio di imputazione a titolo di responsabilità contrattuale *ex art. 1218 c.c.* – che ammette la prova liberatoria con onere a carico del danneggiante, applicabile nell'ordinamento italiano alle ipotesi di responsabilità della struttura sanitaria o del medico libero professionista – a favore del regime di responsabilità a titolo di *strict liability*.

9. IA nel sistema sanitario: da ausilio ad ausiliario

Ad oggi sono moltissime le applicazioni di IA nel campo della medicina e promozione della salute, sia in campo clinico⁹⁴, sia in campo chirurgico⁹⁵, sia mediante l'utilizzo del "gemello digitale"⁹⁶, valido modello artificiale di organo o organismo, per testare le reazioni del paziente reale a interventi e trattamenti.

I sistemi di IA software possono essere utilissimi ausili per la diagnosi delle patologie e la

89. Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale) [COM\(2022\) 496](#).

90. D.lgs. 6 settembre 2005, n. 206.

91. Direttiva [85/374/EEC](#) del Consiglio del 25 luglio 1985 relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri in materia di responsabilità per danno da prodotti difettosi, ancora in vigore nella versione aggiornata.

92. Proposta di Direttiva del Parlamento Europeo e del Consiglio sulla responsabilità per danno da prodotti difettosi [COM\(2022\) 495](#).

93. D'ADDA 2022, p. 836.

94. CHARY-BOYER-BURNS 2021; PILIUK-TOMFORDE 2023; TENG-LIU-SONG et al. 2022.

95. *Ex multis* WANG-GAO-VÁNCZA et al. 2019.

96. POPA-VAN HILTEN-OOSTERKAMP-BOGAARDT 2021.

formulazione delle terapie in modo personalizzato⁹⁷, in considerazione dell'enorme mole di dati che il cervello elettronico ha immagazzinato in fase di addestramento e che può confrontare con la fattispecie concreta in un lasso di tempo minimo. Una delle specialità di maggiore esito riguarda il trattamento del diabete⁹⁸.

I dispositivi medici, dotati di un componente di sicurezza che è un sistema di IA o che sono essi stessi sistemi di IA, sono già oggetto di regolamentazione da parte dei Regolamenti 2017/745 e 2017/746⁹⁹, ricompresi nell'elenco dell'allegato I dell'*AI Act*, sezione A, "Elenco della normativa di armonizzazione" ai nn. 11 e 12.

Nel caso dei dispositivi medici, costituiti anche da un sistema di IA o che sono essi stessi un sistema di IA, può verificarsi un'ipotesi di duplicazione o contraddizione tra norme: quelle della *lex specialis* che prescrive standard di sicurezza e obblighi di valutazione di conformità¹⁰⁰ per i dispositivi medici e quella della *lex generalis* che riguarda i sistemi di IA componenti di sicurezza di un dispositivo medico o che sono essi stessi un dispositivo medico.

Al fine di prevenire una possibile antinomia il legislatore europeo ha statuito:

La classificazione di un sistema di IA come ad alto rischio a norma del presente regolamento non dovrebbe necessariamente significare che il prodotto il cui componente di sicurezza è il sistema di IA, o il sistema di IA stesso in quanto prodotto, sia considerato "ad alto rischio" in base ai criteri stabiliti nella pertinente normativa di armonizzazione dell'Unione che si applica al prodotto. Ciò vale, in particolare, per i regolamenti (UE) 2017/745 e (UE) 2017/746, in cui

è prevista una valutazione della conformità da parte di terzi per i prodotti a medio rischio e ad alto rischio.¹⁰¹

Il Considerando 51 è norma di coordinamento poiché risolve il problema della doppia valutazione di conformità, alla quale sono sottoposti determinati apparecchi utilizzati in ambito sanitario, dotati di componenti di IA: la soluzione dettata dalla legislazione rende indipendenti le due valutazioni che tengono conto di tipologie di rischio differenti e pertanto non necessariamente la qualifica ad alto rischio secondo la normativa speciale dei Regolamenti del 2017 (*Medical Devices Regulations* o MDR) implica la stessa qualificazione nei termini dell'*AI Act*.

Questi particolari sistemi di IA sono assoggettati agli stessi requisiti ed obblighi di tutti gli altri, a seconda che siano inquadrati tra quelli "a rischio alto"¹⁰² o medio/basso.

Per i sistemi ad alto rischio i fornitori, e gli altri soggetti corresponsabili della messa a punto del prodotto finale, devono ottemperare a tutto quanto prescritto dal Capo III del Regolamento, senza possibilità di deroga alla norma generale che richiede la valutazione di conformità, di cui all'art. 43.

Appare degna di menzione la disciplina dell'art. 46, comma 7 che esclude dalla deroga di cui all'art. 43, i sistemi di IA di cui all'allegato I, pur ammettendo in generale che un sistema di IA possa essere messo in commercio o in servizio senza aver superato la procedura di valutazione della conformità, per «motivi di sicurezza pubblica o di protezione della vita e della salute delle persone e di protezione dell'ambiente...»¹⁰³.

97. BRIGANTI-LE MOINE 2020.

98. DEUTSCH-AHLQVIST-ÜDLER 2022.

99. I due regolamenti sono pienamente applicabili dal maggio 2021: Regolamento (Ue) [2017/745](#) del Parlamento Europeo e del Consiglio relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio; Regolamento (Ue) [2017/746](#) del Parlamento Europeo e del Consiglio relativo ai dispositivi medico-diagnostici in vitro e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione.

100. Cfr. art. 5, comma 1 Regolamento (Ue) 2017/745: «Un dispositivo può essere immesso sul mercato o messo in servizio solo se è conforme al presente regolamento qualora sia debitamente fornito e correttamente installato, oggetto di un'adeguata manutenzione e utilizzato conformemente alla sua destinazione d'uso».

101. Considerando 51.

102. Cfr. Considerando 46.

103. Articolo 46.

È da notare che l'art. 59 del Regolamento 2017/745 e l'articolo 54 del Regolamento 2017/746 già prevedevano una deroga alla valutazione di conformità richiesta in base ai rischi specifici di quei settori di attività. Tuttavia, mentre la proposta di legge del 2021¹⁰⁴ consentiva la deroga alla procedura di valutazione della conformità anche per i dispositivi medici dotati di IA¹⁰⁵, la formulazione attuale non permette, in un'ottica tuzioristica, che le autorità competenti autorizzino, seppur motivatamente, l'immissione sul mercato o la messa in servizio, nel territorio dello Stato membro interessato, di dispositivi specifici per i quali le procedure di valutazione di conformità non siano state espletate, neanche se l'impiego fosse «nell'interesse della salute pubblica o della sicurezza o salute dei pazienti».

In particolari situazioni di urgenza la normativa deve bilanciare interessi giuridicamente rilevanti di carattere opposto: da un lato l'esigenza dei pazienti a trattamenti e protocolli sempre più evoluti ed efficaci nel minor tempo possibile, dall'altro l'irrinunciabile funzione di garanzia dell'ordinamento giuridico che prescrive un sistema di verifica dei requisiti e plurimi controlli – che richiedono tempo – prima dell'immissione in circolazione di nuovi dispositivi, per promuovere la sicurezza, affidabilità e protezione dei diritti fondamentali. Da un lato l'interesse della ricerca scientifica all'avanzamento delle conoscenze e delle tecnologie, dall'altra la prospettiva tuzioristica del sistema sanitario che deve minimizzare i rischi per i pazienti e la collettività e autorizzare nuovi trattamenti o tecnologie solo quando le percentuali di rischio per la vita o la salute degli esseri umani siano di gran lunga inferiori rispetto ai possibili benefici; da un lato l'interesse di mercato dell'industria biomedica, dall'altro l'interesse della collettività ad accedere al minimo costo e in condizioni di parità

alle cure ritenute maggiormente efficaci e più sicure allo stato dell'arte.

Altra disposizione specifica riguarda l'obbligo di notifica degli eventi avversi¹⁰⁶, che, in questo caso, riguarda solo quelli gravi.

Quanto agli obblighi di trasparenza, nel settore sanitario si aggiungono alcune osservazioni rispetto a quanto detto per tutti i sistemi di IA.

Per i sistemi di IA utilizzati nel settore sanitario, è auspicabile il massimo dell'accuratezza per ottenere i migliori risultati possibili dall'applicazione, però questo potrebbe compromettere la trasparenza¹⁰⁷. Tuttavia, secondo alcuni studiosi¹⁰⁸ non necessariamente una maggiore spiegabilità riduce l'accuratezza, come a prima vista ritenuto. Infatti, una maggiore interpretabilità o trasparenza potrebbe dar luogo ad una maggiore accuratezza¹⁰⁹, perché una migliore comprensione dell'output dei sistemi di IA da parte dei medici, ad esempio della diagnosi prospettata o terapia proposta, potrebbe rendere più efficace la prassi medica ed anche più accettabile dal paziente.

Non sempre la velocità, disponibilità, precisione, ma anche freddezza, automatismo e spersonalizzazione sono preferiti al rapporto interpersonale di fiducia con il medico.

In ultima analisi tutti i sistemi ad alto rischio sono assoggettati ad una disciplina che impone requisiti e procedure per la certificazione di qualità e sicurezza: eppure non è possibile impedire in assoluto che sistemi di IA, che sono caratterizzati dall'apprendimento automatico, in particolar modo se di IA generativa, evolvano in modo da oltrepassare i paletti imposti dalle norme e di conseguenza ledere determinati diritti fondamentali. Questa possibilità in ambito sanitario potrebbe avere un impatto ancora più negativo.

Se l'intelligenza artificiale modifica le procedure e le sequenze di operazioni in corso d'opera,

104. Articolo 59, comma 1, Regolamento 2017/745.

105. Cfr. art. 47, comma 6 della Proposta di Legge sull'Intelligenza artificiale (2021)206.

106. Articolo 73, comma 10: «Per i sistemi di IA ad alto rischio che sono componenti di sicurezza di dispositivi, o sono essi stessi dispositivi, disciplinati dai regolamenti (UE) 2017/745 e (UE) 2017/746, la notifica è limitata agli incidenti gravi di cui all'articolo 3, punto 44, lettera c), del presente regolamento ed è trasmessa all'autorità nazionale competente scelta a tal fine dagli Stati membri in cui si è verificato l'incidente».

107. D'ELIA 2023.

108. Cfr. HATHERLEY–SPARROW–HOWARD 2023.

109. In questo senso D'ELIA 2023.

divorando non solo dati, ma codici e istruzioni su come formulare i codici, non si può fare affidamento su una certificazione di qualità che attesta la regolarità del sistema ad un certo momento, ma non può assicurarne la sicurezza nel prossimo futuro (c.d. *state of art defence*). In effetti il sistema di gestione dei rischi, come noto, può prevedere solo ciò che accade nel maggior numero di casi o ciò che potrebbe presuntivamente accadere, ma non può tenere conto di esiti di un processo di cui non si conosce la procedura.

Con questa consapevolezza anche lo stesso dettato dell'articolo 9¹¹⁰ potrebbe essere ritenuto oscuro: non appare chiaro come la normativa possa demandare ad un organismo di certificazione una valutazione su qualcosa che effettivamente quest'ultimo non può conoscere ma solo ipotizzare. La stessa espressione "rischi individuati" mira a restringere il campo della gestione del rischio al solo novero di quelli conosciuti, perché potrebbero esservene altri "non individuati", ovvero non conosciuti o conoscibili.

La logica di sistema di gestione del rischio non può soddisfare tutte le esigenze di garanzia e protezione dei diritti, almeno in riferimento ai sistemi di IA caratterizzati dal *deep learning*¹¹¹ e IA generativa, poiché essi sono qualificati proprio dalla non-conoscibilità del possibile futuro sviluppo (fenomeno della c.d. *black-box*). Come la procedura civile insegna, non c'è affidabilità senza spiegabilità, perché una decisione è impugnabile solo sulla base delle motivazioni e non del solo dispositivo. Se la decisione di IA sulla diagnosi, ad esempio, diventa una "sentenza senza motivi", risulta difficile anche solo commentarla perché non se ne comprendono le argomentazioni fondative né il percorso logico che giustifica il disposto finale.

Il legislatore europeo, adottando il *New Legislative Framework*, formula una serie di norme procedurali, quasi un "codice di procedura algoritmica", al quale però sfuggono le sequenze degli agenti

intelligenti artificiali: nel settore sanitario un difetto di *explainability* e *interpretability* potrebbe portare a conseguenze rilevanti, come provocare sfiducia.

10. AI in healthcare: un problema di fiducia

Quanto fin qui detto conduce la riflessione ad alcune considerazioni finali.

L'utilizzo delle applicazioni di IA in medicina può apportare benefici ed opportunità enormi in termini di supporto alle attività diagnostiche, terapeutiche, chirurgiche e sanitarie in generale. Ai vantaggi si affiancano alcune questioni bioetiche¹¹² e biogiuridiche analoghe a quelle che sono sollevate dall'adozione di qualsiasi tipo di tecnologia nel campo della cura e promozione della salute umana: la questione del bilanciamento dello sviluppo scientifico e dell'innovazione tecnologica con il rispetto della dignità della vita umana, dal concepimento alla morte naturale e dei suoi diritti fondamentali.

La problematica specifica dei sistemi di IA nel settore sanitario è indotta da una distorsione dovuta alla prospettiva del riduzionismo scientifico, che annulla la dimensione personale nella relazione di cura e prospetta di sostituire il medico e le sue attività, l'esame obiettivo e le sue valutazioni in scienza e coscienza¹¹³, con algoritmi seppur sofisticatissimi.

La relazione di cura è un problema di fiducia¹¹⁴ oltre che di comprensione intellettuale della patologia, e non si può avere fiducia in una sequenza algoritmica, della quale neanche si conosce il procedimento argomentativo¹¹⁵.

In una prospettiva biogiuridica, è indispensabile che tutti i sistemi di IA, che si collocano nelle diverse fasi del procedimento clinico o chirurgico, lascino spazio ad una ponderazione dell'uomo-medico in tutte le fasi decisionali del processo, anche al fine di garantire il consenso informato¹¹⁶ al paziente sulla base di un'autentica

110. Si veda il comma 2 dell'articolo 9.

111. Sul punto cfr. MESSINA 2023, pp. 248-253.

112. GOLDBERG-ADAMS-BLUMENTHAL et al. 2024.

113. Cfr. MELINA 2018.

114. POWELL 2019.

115. FELDMAN-ALDANA-STEIN 2019.

116. DAVERIO 2023.

comprensione della prescrizione o terapia che gli viene proposta¹¹⁷.

L'esercizio della professione medico-sanitaria è incompatibile con l'automatizzazione assoluta delle decisioni e la delega in bianco delle determinazioni, sui trattamenti da adottare o sugli interventi da eseguire, ad un calcolatore elettronico. Il medico e tutti coloro, che sono coinvolti nelle relazioni di cura e di assistenza, non possono abdicare alla

responsabilità¹¹⁸ delle scelte, che sono allo stesso tempo scientifiche e prudenziali, nei confronti di un sistema di IA prodotto dall'uomo.

Come sottolineato già dai bioeticisti, al fine di tutelare la dignità personale dell'uomo, sia del paziente che del medico, è necessario rimettere al centro della prassi e della normazione la persona umana¹¹⁹ e la sua libertà, senza cedere il controllo ad un altro timoniere¹²⁰.

Riferimenti bibliografici

- S.M. ALHASHMI, I.A.T. HASHEM, I. AL-QUDAH (2024), *Artificial Intelligence applications in healthcare: A bibliometric and topic model-based analysis*, in "Intelligent Systems with Application", vol. 21, 2024, n. 3
- A.C. AMATO MANGIAMELI (2023), *Intelligenza artificiale*, in A.C. Amato Mangiameli, G. Saraceni (a cura di), "Cento e una voce di informatica giuridica", Giappichelli, 2023
- A.C. AMATO MANGIAMELI (2022), *Intelligenza artificiale*, in E. Sgreccia, A. Tarantino (diretto da), "Enciclopedia di Bioetica e Scienza Giuridica", Aggiornamento vol. I, Edizioni Scientifiche Italiane, 2022
- A.C. AMATO MANGIAMELI (2022-A), *Intelligenza artificiale, big data e nuovi diritti*, in "Rivista italiana di informatica e diritto", 2022, n. 1
- H. ARENDT (2004), *Responsabilità e giudizio*, trad. it., Einaudi, 2004
- J. BALI, R. GARG, R.T. BALI (2019), *Artificial Intelligence (AI) in healthcare and biomedical research: Why a strong computational/AI bioethics framework is required?*, in "Indian Journal of Ophthalmology", vol. 67, 2019, n. 1
- A. BARRACCA, S. LEDDA, G. MANCOSU et al. (2017), *La medicina fra intelligenza artificiale e necessità di un nuovo Umanesimo*, in "Giornale di clinica nefrologica e dialisi", vol. 29, 2017, n. 3
- T. BAYNE, A. CLEEREMANS, P. WILKEN (eds.) (2009), *The Oxford Companion to Consciousness*, Oxford University Press, 2009
- R.M. BELLINO (2015), *Medicina*, in E. Sgreccia, A. Tarantino (diretto da), "Dizionario di Bioetica e Scienza Giuridica", vol. VIII, Edizioni Scientifiche Italiane, 2015
- A. BERLEJUNG, C. FREVEL (a cura di) (2009), *I concetti teologici fondamentali dell'Antico e del Nuovo Testamento*, trad. it., Queriniana, 2009

117. MESSINETTI 2019.

118. Come ricordava Hannah Arendt, abdicare alla propria coscienza ed alla facoltà di giudizio in favore di un potere esterno o del parere già formulato dalla maggioranza è una tentazione ricorrente, soprattutto sotto i regimi totalitari: «Tante sono le ragioni per le quali il problema del diritto e della capacità di giudizio investe questioni morali di primissima importanza ... Primo, come posso distinguere ciò che è giusto da ciò che è sbagliato quando la maggioranza o la totalità delle persone che mi stanno accanto ha già formulato un giudizio? ... E in effetti esiste, nella nostra società, una diffusa paura di giudicare, una paura che non ha nulla a che fare con il detto biblico "Non giudicare se non vuoi essere giudicato" ... In realtà, dietro il non volere giudicare si cela il dubbio che nessuno sia libero, il dubbio che nessuno sia responsabile o possa rispondere degli atti che ha commesso», cfr. ARENDT 2004, pp. 16-17.

119. PALAZZANI 2022.

120. Κυβερνήτης = timoniere, in greco.

- G. BRIGANTI, O. LE MOINE (2020), *Artificial Intelligence in Medicine: Today and Tomorrow*, in “Frontiers in Medicine”, vol. 7, 2020
- C. CAMPIGLIO (2023), *Giurisdizione e legge applicabile in materia di responsabilità medica (ovvero, a proposito di conflitti di qualificazioni)*, in “Rivista di diritto internazionale privato e processuale”, 2023, n. 4
- G. CASSANO, S. PREVITI (a cura di) (2020), *Il diritto di Internet nell'era digitale*, Giuffrè, 2020
- G. CERRINA FERONI (2023), *Intelligenza artificiale e sistemi di scoring sociale. Tra distopia e realtà*, in “Diritto dell'Informazione e dell'informatica”, 2023, n. 1
- M. CHARY, E.W. BOYER, M.M. BURNS (2021), *Diagnosis of acute poisoning using explainable artificial intelligence*, in “Computers in Biology and Medicine”, vol. 134, 2021
- E. COLLETTI (2021), *Intelligenza artificiale e attività sanitaria. Profili giuridici dell'utilizzo della robotica in medicina*, in “Rivista di diritto dell'economia, dei trasporti e dell'ambiente”, vol. XIX, 2021
- COMITATO NAZIONALE PER LA BIOETICA (2020), *Intelligenza artificiale e medicina: aspetti etici*, 29 maggio 2020
- CONSIGLIO SUPERIORE DI SANITÀ - MINISTERO DELLA SALUTE (2023), *Linee guida, percorso diagnostico-terapeutico-assistenziale (PDTA), sviluppi e prospettive della Chirurgia robotica nel SSN e riflessioni sul Knowledge Transfer dell'Intelligenza Artificiale (IA)*, 13 febbraio 2023
- CONSIGLIO SUPERIORE DI SANITÀ - MINISTERO DELLA SALUTE (2021), *I sistemi di intelligenza artificiale come strumento di supporto alla diagnostica*, 9 novembre 2021
- J. COWBURN (2013), *Scientism: a word we need*, Mosaic Press, 2013
- A. D'ADDA (2022), *Danni «da robot» (specie in ambito sanitario) e pluralità di responsabili tra sistema della responsabilità civile ed iniziative di diritto europeo*, in “Rivista di diritto civile”, 2022, n. 3
- C. D'Elia (2023), *Gli strumenti di intelligenza artificiale generativa nel contesto sanitario: problemi di ottimizzazione delle risorse e questioni di spiegabilità*, in “Rivista italiana di medicina legale e del diritto in campo sanitario”, 2023, n. 1
- M. DAVERIO (2023), *Informed Consent and Medical Decision-Making Applying Artificial Intelligence. Ethical Aspects and Implications for the Doctor-Patient Relationship*, in “Rivista di filosofia del diritto”, 2023, n. 2
- M. DAVERIO, F. MACIOCE (2023), *Intelligenza artificiale e diritto alla salute nella regolazione europea: aspetti emergenti riguardo alla relazione medico-paziente*, in “Teoria e Critica della Regolazione Sociale”, 2023, n. 1
- A.J. DEUTSCH, E. AHLQVIST, M.S. UDLER (2022), *Phenotypic and genetic classification of diabetes*, in “Diabetologia”, vol. 65, n. 2022
- EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES (2018), *Statement on artificial intelligence, robotics and 'autonomous' systems*, Brussels, 9 March 2018
- R.C. FELDMAN, E. ALDANA, K. STEIN (2019), *Artificial Intelligence in the Health Care Space: How We Can Trust What We Cannot Know*, in “Stanford Law & Policy Review”, vol. 30, 2019
- E.A. FERIOLI (2019), *L'intelligenza artificiale nei servizi sociali e sanitari: una nuova sfida al ruolo delle istituzioni pubbliche nel welfare italiano?*, in “BioLaw Journal – Rivista di BioDiritto”, 2019, n. 3
- G. FINOCCHIARO (2022), *La regolazione dell'intelligenza artificiale*, in “Rivista trimestrale di diritto pubblico”, 2022, n. 3
- V. FRANCESCHELLI (2023), *Sull'intelligenza artificiale (IA o AI)*, in “Rivista di diritto industriale”, 2023, n. 1

- FRANCESCO (2022), *Discorso del Santo Padre Francesco ai membri della Federazione delle Associazioni Familiari Cattoliche in Europa*, 10 giugno 2022
- C. FREVEL (2009), *Cuore*, in A. Berlejung, C. Frevel (a cura di), "I concetti teologici fondamentali dell'Antico e del Nuovo Testamento", trad. it., Queriniana, 2009
- E. GABRIELLI, U. RUFFOLO (2019), *Introduzione alla sezione "Intelligenza Artificiale e diritto"*, in "Giurisprudenza italiana", 2019, n. 7
- S. GALLAGHER, D. ZAHAVI (2009), *La mente fenomenologica*, Raffaello Cortina Editore, 2009
- M. GANDOLFINI (2013), *I volti della coscienza*, Cantagalli, 2013
- C.B. GOLDBERG, L. ADAMS, D. BLUMENTHAL et al. (2024), *To do no harm – and the most good – with AI in health care*, in "Nature Medicine", vol. 30, 2024
- A.G. GRASSO (2023), *Diagnosi algoritmica errata e responsabilità medica*, in "Rivista di diritto civile", 2023, n. 2
- J. HATHERLEY, R. SPARROW, M. HOWARD (2023), *The Virtue of Interpretable Medical AI*, in "Cambridge Quarterly of Healthcare Ethics", 2023
- J. HE, S.L. BAXTER, J. XU et al. (2019), *The practical implementation of artificial intelligence technologies in medicine*, in "Nature medicine", vol. 25, 2019, n. 1
- P.B. HELZEL (2021), *La vulnerabilità del rapporto medico-paziente nell'era delle tecnologie emergenti*, in "L'Ircocervo", vol. 20, 2021, n. 2
- HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (2020), *The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*, Publications Office of the European Union, 2020
- HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (2019), *Ethics guidelines for trustworthy AI*, Publications Office of the European Union, 2019.
- HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (2019-A), *Policy and investment recommendations for trustworthy AI*, Publications Office of the European Union, 2019
- J. IQBAL, D.C. CORTÉS JAIMES, P. MAKINENI et al. (2023), *Reimagining Healthcare: Unleashing the Power of Artificial Intelligence in Medicine*, in "Curēus", vol. 15, 2023, n. 9
- JOINT RESEARCH CENTRE (2020), *AI Watch. Artificial Intelligence in Medicine and Healthcare: applications availability and societal impact*, Publications Office of the European Union, 2020
- S.M. KAMPOWSKI (2010), *Una libertà più grande: la biotecnologia, l'amore e il destino umano*, Cantagalli, 2010
- R. KHERA, A.J. BUTTE, M. BERKWITS et al. (2023), *AI in Medicine – JAMA's Focus on Clinical Outcomes, Patient-Centered Care, Quality and Equity*, in "Journal of the American Medical Association", vol. 330, 2023, n. 9
- E. LEPORE, A. PYLYSHYN (eds.) (1999), *What is cognitive science?*, Blackwell, 1999
- L.M. LUCARELLI TONINI (2023), *L'IA tra trasparenza e nuovi profili di responsabilità: la nuova proposta di "AI liability directive"*, in "Il Diritto dell'informazione e dell'informatica", 2023, n. 2
- B. MAIER, W.A. SHIBLES (2011), *The Philosophy and Practice of Medicine and Bioethics. A Naturalistic-Humanistic Approach*, Springer, 2011
- J. MCCARTHY, M.L. MINSKY, N. ROCHESTER, C.E. SHANNON (2006), *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955*, in "AI Magazine", vol. 27, 2006, n. 4
- L. MELINA (2018), *Coscienza e prudenza*, Cantagalli, 2018

- D. MESSINA (2023), *La tutela della dignità nell'era digitale*, Edizioni Scientifiche Italiane, 2023
- R. MESSINETTI (2019), *La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in "Contratto e impresa", 2019, n. 3
- A. MISHRA, J. SAVULESCU, A. GIUBILINI (2021), *The Ethics of Medical AI*, in C. Véliz (ed.), "The Oxford Handbook of Digital Ethics", Oxford University Press, 2021
- B. MITTELSTADT (2022), *The impact of Artificial Intelligence in the doctor-patient relationship*, European Council, 2022
- D. MORANA, T. BALDUZZI, F. MORGANTI (2022), *La salute "intelligente": eHealth, consenso informato e principio di non-discriminazione*, in "federalismi.it", 2022, n. 34
- N. MUSACCHIO, G. GUAITA, A. OZZELLO et al. (2018), *Intelligenza Artificiale e Big Data in ambito medico: prospettive, opportunità, criticità*, in "JAMD – The Journal of AMD", vol. 21, 2018, n. 3
- A. NOË (2010), *Perché non siamo il nostro cervello: una teoria radicale della coscienza*, Raffaello Cortina Editore, 2010
- L. PALAZZANI (2022), *Technological humanism: a philosophical framework for education*, in "Archivio giuridico", 2022, n. 3
- L. PALAZZANI (2021), *AI and Health: Ethical Aspects for Regulation*, in "Teoria e critica della regolazione sociale", 2021, n. 1
- L. PALAZZANI, S. ZANNOTTI (a cura di) (2013), *Il diritto delle neuroscienze. Non "siamo" i nostri cervelli*, Giappichelli, 2013
- A.-D.E. PAREKH, O.A. SHAIKH, SIMRAN et al. (2023), *Artificial intelligence (AI) in personalized medicine: AI-generated personalized therapy regimens based on genetic and medical history: short communication*, in "Annals of Medicine and Surgery", vol. 85, 2023, n. 11
- A. PASCUAL LEONE, A. AMEDI, F. FREGNI, L.B. MERABET (2005), *The plastic human brain cortex*, in "Annual Review of Neuroscience", vol. 28, 2005
- K. PILIUK, S. TOMFORDE (2023), *Artificial Intelligence in Emergency Medicine. A Systematic Literature Review*, in "International Journal of Medical Informatics", vol. 180, 2023, n. 6
- E.O. POPA, M. VAN HILTEN, E. OOSTERKAMP, M.-J. BOGAARDT (2021), *The use of digital twins in healthcare: socio-ethical benefits and socio-ethical risks*, in "Life Sciences, Society and Policy", vol. 17, 2021, n. 6
- J. POWELL (2019), *Trust Me, I'm a Chatbot: How Artificial Intelligence in Health Care Fails the Turing Test*, in "Journal of Medical Internet Research", vol. 21, 2019, n. 10
- Z. PYLYSHYN (1999), *What's in Your Mind?*, in E. Lepore, Z. Pylyshyn (eds.), "What is cognitive science?", Blackwell, 1999
- U. RUFFOLO (2021), *L'Intelligenza artificiale in sanità: dispositivi medici, responsabilità e "potenziamento"*, in "Giurisprudenza italiana", 2021, n. 2
- U. RUFFOLO (2021-A), *Le "mobili frontiere" della responsabilità medica*, in "Giurisprudenza italiana", 2021, n. 2
- S. RUSSELL, P. NORVIG (2021), *Intelligenza artificiale. Un approccio moderno*, Pearson, 2021
- G. SALITO (2022), *La responsabilità da algoritmo tra (teoria della) finzione e realtà sanitaria: una nuova declinazione della responsabilità medica?*, in "Rivista italiana di medicina legale e del diritto in campo sanitario", 2022, n. 4

- V. SALVATORE (a cura di) (2023), *Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea*, Giappichelli, 2023
- G. SARTOR (2022), *L'intelligenza artificiale e il diritto*, Giappichelli, 2022
- G. SARTOR (2002), *Gli agenti software: nuovi soggetti del ciberdiritto?*, in "Contratto e impresa", vol. 18, 2002, n. 2
- J.R. SEARLE (1984), *Menti, cervelli e programmi*, trad. it., Clup-Clued, 1984
- Y. SONG, B. MILLIDGE, T. SALVATORI et al. (2024), *Inferring neural activity before plasticity as a foundation for learning beyond backpropagation*, in "Nature Neuroscience", vol. 27, 2024
- R. SPAEMANN (2013), *Essere persone*, La Scuola, 2013
- G. TADDEI ELMÌ (2020), *Soggettività e responsabilità dei sistemi di IA*, in G. Cassano, S. Previti (a cura di), "Il diritto di Internet nell'era digitale", Giuffrè, 2020
- Q. TENG, Z. LIU, Y. SONG et al. (2022), *A survey on the interpretability of deep learning in medical diagnosis*, in "Multimedia System", vol. 28, 2022
- A.E. TOZZI (2023), *Verso una leadership clinica dell'intelligenza artificiale per la salute*, in "L'Endocrinologo", vol. 24, 2023, n. 5
- A.M. TURING (1950), *Computing machinery and intelligence*, in "Mind", vol. 59, 1950, n. 236 (disponibile nella traduzione italiana a cura di G. Lolli, A.M. TURING, *Intelligenza meccanica*, trad. it., Bollati Boringhieri, Torino 1994)
- UNESCO (2021), *Recommendation on Ethics of Artificial Intelligence*, 23rd November 2021
- UNESCO (2017), *Report of the International Bioethics Committee on Big Data and Health*, 15th September 2017
- UNESCO (2005), *Universal Declaration on Bioethics and Human Rights*, 2005
- L. WANG, R. GAO, J. VÁNCZA et al. (2019), *Symbiotic human-robot collaborative assembly*, in "Manufacturing Technology", vol. 68, 2019
- WORLD HEALTH ORGANIZATION (2021), *Ethics and governance of artificial intelligence for health: WHO guidance*, 2021
- N. XU, D. YANG, K. ARIKAWA, C. BAI (2023), *Application of artificial intelligence in modern medicine*, in "Clinical eHealth", vol. 6, 2023, n. 12



RICCARDO MICHELE COLANGELO

Ne pereant fragmenta: l'intelligenza artificiale e la complessità della Corptech governance

Il crescente utilizzo delle tecnologie digitali nell'esercizio di attività d'impresa comporta significative questioni di cyberdiritto societario. Anche nello specifico ambito dei c.d. rischi tecnologici d'impresa, l'apporto dell'informatica giuridica e l'approccio metodologico del giurista informatico possono agevolare un'indagine più completa degli elementi di complessità che caratterizzano le nuove tecnologie, agevolando al contempo l'adeguatezza degli assetti societari. A margine della definitiva approvazione dell'AI Act, il presente contributo intende approfondire tali considerazioni in tema di *Corptech governance*, con particolare riguardo all'uso di sistemi di intelligenza artificiale, evidenziando anche profili di *data protection* e sicurezza informatica, nonché le ricadute sugli assetti. Lungi dalle logiche di una mera opera ricognitiva, si intende sottolineare l'esigenza di superare l'approccio formalistico talora emergente in sede di *compliance* normativa, valorizzando il ruolo degli assetti digitali ed aprendo la via ad una non procrastinabile attenzione ai profili di *Corporate Digital Responsibility*.

*Intelligenza artificiale – Corptech governance – Informatica giuridica – Assetti societari
Corporate Digital Responsibility*

Ne pereant fragmenta: artificial intelligence and the complexity of Corptech governance

The rise in the use of digital technologies in business activities brings up significant issues about corporate cyberlaw. Also in the specific field of the so-called technological risks of business, legal informatics and IT jurist's methodological approach can enable a broader examination of the complexity associated with new technologies, while facilitating the adequacy of corporate structures. After a brief period following the final approval of the AI Act, this paper intends to deepen these relevant issues regarding Corptech governance, focusing on the use of artificial intelligence systems and highlighting data protection and cybersecurity concerns, along with the impact on corporate structures. This paper also aims to emphasise the need to overcome the formalistic approach sometimes arising in the context of regulatory compliance, paving the way for an unpostponable focus on Corporate Digital Responsibility.

*Artificial intelligence – Corptech governance – Legal informatics – Corporate structures
Corporate Digital Responsibility*

SOMMARIO: 1. Attività d'impresa e tecnologie digitali. – 2. Il giurista informatico e l'intelligenza artificiale. – 3. Brevi note sui profili giuridici di complessità dell'IA. – 3.1. *Dalla data protection...* – 3.2. *...alla sicurezza informatica.* – 4. Alcuni spunti circa l'adeguatezza degli assetti digitali. – 5. Il ruolo della *Corporate Digital Responsibility*.

1. Attività d'impresa e tecnologie digitali

Il crescente ricorso, nell'ambito dell'esercizio collettivo di attività d'impresa, all'utilizzo delle tecnologie digitali, ancora oggi caratterizzato da ampi margini di perfettibilità e fortemente auspicato e stimolato anche a livello eurounitario, non può essere apprezzato appieno, nei suoi risvolti giuridici, limitandosi ad analisi quantitative e ad osservazioni meramente fattuali¹.

Queste ultime, d'altra parte, sebbene talora condizionate da alcuni vincoli metodologici non

del tutto condivisibili, consentono quantomeno di stimare, grazie a dati statisticamente rilevanti, la concreta diffusione di determinate tecnologie nello specifico contesto societario².

Pur prescindendo dai profili eminentemente quantitativi, l'impiego di tecnologie digitali – che talora viene percepito quale vero e proprio limite all'avvio di una nuova attività imprenditoriale³ – risulta di norma caratterizzato da non pochi corollari giuridicamente rilevanti, continuando a porre, per quanto interessa maggiormente in questa sede, stimolanti questioni di cyberdiritto societario.

1. Sia sufficiente, in proposito, il rimando all'ultimo (e primo) *Report on the state of the Digital Decade 2023*, pubblicato dalla Commissione europea nel mese di settembre 2023 (cfr. EUROPEAN COMMISSION 2023-A) e che *de facto* subentra al *Digital Economy and Society Index* (DESI), ove non emergono dati particolarmente lusinghieri circa l'attuale ricorso alle tecnologie in ambito societario, in modo speciale per quanto concerne le PMI. Il Rapporto è stato introdotto dalla Decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio del 14 dicembre 2022, che istituisce il programma strategico per il decennio digitale 2030. Per quanto maggiormente interessa in questa sede, la decisione *de qua*, all'art. 4, par. 1, n. 3, prevede specifici obiettivi in materia di «trasformazione digitale delle imprese»: il ricorso, da parte di «almeno il 75 % delle imprese dell'Unione, in base alle proprie esigenze aziendali», alternativamente a servizi di cloud computing, big data e/o intelligenza artificiale; il raggiungimento quantomeno di un «livello base di intensità digitale» da parte di «oltre il 90% delle PMI dell'Unione»; l'agevolazione da parte dell'Ue di «scale-up innovative» favorendo «il loro accesso ai finanziamenti, almeno raddoppiando il numero di aziende unicorni». In dottrina, per tutti, si vedano MATRICANO 2020 e PASCUCCI 2017, p. 5 ss.
2. Nel *Report on the state of the Digital Decade 2023. Annex Italy*, con particolare riguardo ai dati concernenti il contesto italiano, risulta preso in considerazione l'utilizzo di tecnologie digitali «avanzate» e, in relazione ai soli sistemi di intelligenza artificiale, si quantifica nella misura del 6% la quota di società che vi hanno fatto ricorso nel 2021: cfr. EUROPEAN COMMISSION 2023-B. Più articolata, invece, la *Rilevazione sulle tecnologie dell'informazione e della comunicazione (Ict)* dell'ISTAT, pubblicata il 4 gennaio 2023 e riferita all'anno precedente, che tuttavia non contempla indicatori non secondari, quali «intelligenza artificiale e big data», in quanto, «ad oggi, demandati ad altre fonti di statistica non ufficiale» (così ISTAT 2023, p. 18).
3. Cfr. UNIONCAMERE – ANPAL 2023, pp. 26, 65 e 102. Più in generale, in merito alla propensione imprenditoriale ed all'avvio di nuove imprese, si rinvia ai dati riportati in MICOZZI 2024.

Queste ultime, da un lato, hanno la potenzialità di interrogare, in ultima analisi, anche taluni principi fondamentali della disciplina di settore; dall'altro, non necessariamente coinvolgono *in toto*, e quindi in modo esclusivo e diretto, specifici istituti del diritto commerciale. In argomento, limitando l'analisi ai profili giuridicamente rilevanti, meritano un'adeguata (ri)valutazione anche quelli che indirettamente – ma non in via secondaria – riguardano l'ambito societario, caratterizzati peraltro da risvolti evidenziabili anche in un'ottica di *risk management*⁴, così come informatico-giuridica.

2. Il giurista informatico e l'intelligenza artificiale

In argomento, se è vero che una qualificata attenzione dottrinale allo studio dei fenomeni tecnologici non costituisce più appannaggio del tradizionale settore informatico-giuridico, l'approccio metodologico proprio del giurista informatico, attento a cogliere e valorizzare la rilevanza anche di profili interdisciplinari⁵, consente a tutt'oggi, anche in ambiti specifici come quello del diritto societario, non solo di ampliare il campo dell'analisi, ma anche – e soprattutto – di indagare più compiutamente quegli elementi di complessità che, agli occhi del giurista, caratterizzano le nuove tecnologie⁶.

Tali considerazioni, riferibili al ricorso tanto all'intelligenza artificiale – tema particolarmente attuale, significativamente attenzionato dalla più recente dottrina⁷ – quanto ad altre tecnologie digitali, siano esse strumento o oggetto di governo dell'impresa⁸, risultano preziose nell'ambito della *Corptech governance*⁹, consentendo non solo di apprezzare meglio talune singole tessere, ma anche di scorgere intere porzioni dell'ideale mosaico del cyberdiritto societario. Il tutto con ricadute effettive a beneficio dell'organo gestorio, ai fini di una corretta – e non parziale – strutturazione degli assetti societari, con particolare riguardo a quelli digitali¹⁰, senza sottostimare quanto pertiene non solo alla valutazione dei rischi, ma anche – e soprattutto – alla gestione dei medesimi.

3. Brevi note sui profili giuridici di complessità dell'IA

Più nello specifico, i preconizzati profili di complessità possono scaturire tanto dalla concreta applicabilità, sia essa alternativa o concorrente, di plurime discipline specifiche¹¹, quanto da vuoti normativi relativi all'utilizzo di strumenti informatici di uso ormai corrente. In argomento, oltre alla contingente assenza di disciplina positiva, peraltro non aliena al rapporto tra diritto e nuove tecnologie, caratterizzato di norma da un fisiologico ritardo

4. Tra la più autorevole dottrina giuridica in tema di *risk management* e tecnologie digitali si veda, per tutti, CERRATO 2019.

5. Cfr. BORRUSO-RUSSO-TIBERI 2009, p. 2.

6. In argomento, si consenta di evocare la rilevanza dell'"approccio informatico-giuridico *by design*", proposto in COLANGELO 2023, p. 115.

7. *Ex multis*, e senza pretese di completezza, cfr. BIANCHINI-GASPARRI-RESTA et al. 2022; SCHNEIDER 2022, p. 711 ss.; ABRIANI-SCHNEIDER 2021; MOSCO 2019, p. 247 ss.; ENRIQUES-ZETZSCHE 2019.

8. Cfr. ABRIANI-SCHNEIDER 2021, p. 191 ss. e 235 ss.

9. Cfr. LIBERANOME 2022, p. 94 e SCARCHILLO 2019, p. 881 ss.

10. In argomento, si veda il riferimento agli "assetti cibernetici" riportato in CERRATO-CULASSO-CROCCO 2023, pp. 318-319.

11. Si pensi, in argomento, all'emblematico caso dei criptoasset ed alla limitata portata del regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività (meglio noto con l'acronimo inglese MiCAr), che, all'art. 2, par. 4, riconosce *expressis verbis* l'esclusione dall'ambito di applicazione del regolamento medesimo di un novero piuttosto ampio "cripto", se ed in quanto queste ultime integrano fattispecie già oggetto di una specifica disciplina. A titolo esemplificativo, è questo il caso – certamente non "di scuola" – delle cripto-attività che rientrano nella definizione di strumenti (*rectius*: prodotti) finanziari, in relazione alle quali il successivo comma 5 prevede, entro il 30 dicembre 2024, l'elaborazione, da parte dell'ESMA, di «orientamenti conformemente all'articolo 16 del Regolamento (UE) n. 1095/2010 sulle condizioni e sui criteri per la qualificazione delle cripto-attività come strumenti finanziari».

del legislatore¹² – ben possono assumere rilevanza anche i casi in cui l'iter normativo, seppur avviato, non si sia ancora concluso, così come quelli, non infrequenti soprattutto nel contesto delle fonti di secondo livello del diritto unionale, caratterizzati da una significativa *vacatio*, talora biennale, tra l'entrata in vigore e la concreta applicabilità di una determinata disciplina¹³.

Ciò risulta particolarmente evidente anche operando una sorta di *actio finium regundorum* relativamente all'oggetto delle presenti note, prendendo in considerazione il peculiare e fertile campo dei sistemi di intelligenza artificiale.

Tale ambito, infatti, è risultato a lungo caratterizzato dall'assenza di una disciplina specifica, nelle more della definitiva approvazione del regolamento europeo in materia, noto come AI Act¹⁴.

D'altra parte, l'entrata in vigore di quest'ultimo, intervenuta poco prima della definitiva chiusura delle presenti note, ha per ora consacrato una disciplina che solo gradualmente potrà essere considerata vincolante e, in quanto tale, incidere sullo sviluppo e sull'utilizzo di sistemi di intelligenza artificiale: infatti, il regolamento (UE) 2024/1689 del 13 giugno 2024, pubblicato il successivo 12

luglio¹⁵ ed entrato in vigore venti giorni dopo, sarà pienamente applicabile, nella sua interezza, solo il 2 agosto 2027¹⁶.

Cionondimeno, l'attuale assenza di uno specifico *corpus* di norme giuridiche vincolanti in materia di intelligenza artificiale non può giustificare – in special modo nel contesto dell'adozione di siffatta tecnologia in ambito societario – un entusiastico ma semplicistico “*Omnia licent!*”¹⁷, foriero di una potenziale significativa esposizione a rischi e a responsabilità.

Seppur in assenza di cogenti obblighi normativi, lo stato sempre più avanzato dell'iter legislativo dell'AI Act, culminato con la recentissima approvazione e la successiva entrata in vigore, evidenzia con singolare chiarezza la crescente opportunità di non sottovalutare, in un'ottica proattiva, quantomeno le direttrici della normativa specifica.

Queste ultime, ad onor del vero, avrebbero già potuto essere prese in considerazione – in attesa della pubblicazione del testo definitivo – per come desumibili in concreto dalla disamina dei rilevanti emendamenti alla proposta di AI Act approvati dal Parlamento europeo nel mese di giugno 2023¹⁸, così come dell'ancor più attendibile testo

12. *Ex multis*, cfr. PIETRANGELO 2007, p. 176, ove peraltro si evidenziano anche i principali profili problematici di tale tendenziale ritardo, e ROLLI 2018, pp. XVIII-XIX.

13. Cfr. art. 297 TFUE. Una *vacatio* biennale caratterizza in concreto l'applicabilità del Regolamento generale sulla protezione dei dati personali (2016/679 del 27 aprile 2016), noto con l'acronimo inglese GDPR: entrato in vigore nel 2016, il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea, è divenuto pienamente applicabile solo il 25 maggio 2018, come espressamente previsto ex art. 99, parr. 1 e 2.

14. Commissione europea, Proposta di regolamento del parlamento europeo e del consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione, COM(2021) 206.

15. Si tratta del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (regolamento sull'intelligenza artificiale).

16. Ai sensi dell'art. 113, pur essendo disposta *expressis verbis* la piena applicabilità del regolamento a decorrere dal 2 agosto 2026, sono previste alcune eccezioni, che anticipano – e, in un caso, posticipano – l'applicabilità di alcune norme dell'AI Act. Tali deroghe risultano così formulate alle lettere a)-c): «a) I capi I e II si applicano a decorrere dal 2 febbraio 2025; b) Il capo III, sezione 4, il capo V, il capo VII, il capo XII e l'articolo 78 si applicano a decorrere dal 2 agosto 2025, ad eccezione dell'articolo 101; c) L'articolo 6, paragrafo 1, e i corrispondenti obblighi di cui al presente regolamento si applicano a decorrere dal 2 agosto 2027».

17. “*Omnia licent!*”. *Sed non omnia expediunt. “Omnia licent!”. Sed non omnia aedificant*» (1 Cor 10,23). In dottrina, in senso sostanzialmente conforme, cfr. BORRUSO–RUSSO–TIBERI 2009, p. 582, ove si evidenziano gli “ingenui entusiasmi” talora connaturati all'adozione delle tecnologie informatiche.

18. Parlamento europeo, **emendamenti**, approvati il 14 giugno 2023, alla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione (COM(2021)206 – C9-0146/2021 – 2021/0106(COD)).

consolidato in esito alla risoluzione legislativa del Parlamento europeo del 13 marzo 2024¹⁹.

A ciò si aggiunga un ulteriore – e fondamentale – rilievo: fatta salva la doverosa ed indiscussa applicazione delle norme dell'AI Act a far data da quando, progressivamente, diverranno del tutto vincolanti, le finestre di non applicabilità della nuova disciplina – in maniera non dissimile dalla precedente assenza del quadro normativo specifico in materia di intelligenza artificiale – non possono costituire un'esimente per quanto attiene all'applicazione di quelle ulteriori e differenti norme già in vigore, siano esse di matrice eurounitaria o meno, che, pur non dettate con diretto ed esclusivo riguardo ai sistemi di intelligenza artificiale, possono – *rectius*: debbono – comunque trovare applicazione anche in relazione al corretto utilizzo di questi ultimi, nelle grandi imprese così come nelle PMI.

3.1. Dalla *data protection*...

È questo il caso della normativa vigente in materia di *data protection*: con particolare riguardo al GDPR, è possibile affermare, in prima approssimazione, come il medesimo risulti *ex se* applicabile ai trattamenti di dati personali posti in essere nell'ambito dell'esercizio collettivo di attività d'impresa²⁰.

Più specificamente, non è dato dubitare circa l'applicabilità del Regolamento generale sulla protezione dei dati anche a quei trattamenti caratterizzati dal ricorso a sistemi di intelligenza artificiale²¹, sebbene questi ultimi, all'interno del GDPR, non siano oggetto di alcun espresso ed univoco riferimento testuale.

Di converso, e sempre argomentando *de iure condito*, l'AI Act racchiude in sé, complessivamente, 30 espressi rinvii al GDPR, di cui 14 nei considerando e nelle relative note, altrettanti nell'articolato

e 2 negli allegati, peraltro senza significative variazioni rispetto al precedente testo provvisorio, consolidato in esito agli emendamenti approvati dal Parlamento europeo.

Sul punto, in un'ottica diacronica, è dato osservare una crescita di siffatti riferimenti, laddove il dato quantitativo appena illustrato risulta maggiore rispetto non solo agli sparuti riferimenti al GDPR presenti nel testo originario della proposta di AI Act, ma anche alle 21 ricorrenze rinvenibili negli emendamenti approvati nel mese di giugno 2023.

Tra i riferimenti espressi al regolamento (UE) 2016/679, molti risultano operati all'interno di considerando e riferiti, in gran parte, ai dati biometrici.

Guardando all'articolato vero e proprio, emergono anche riferimenti a specifici istituti, già in precedenza definiti *ex art.* 4 GDPR. Tra di essi, nel vigente AI Act – così come nel testo della proposta di regolamento, come emendata nel 2024 – spiccano quelli riferiti ai dati biometrici (richiamati dall'art. 3, par. 1, punto 34), alle categorie particolari di dati personali (punto 37) ed alla profilazione (punto 52). Risultano, inoltre, riscontrabili anche le definizioni *per relationem* di dati personali e non personali, rispettivamente riportate ai punti 50 e 51 del medesimo art. 3, par. 1.

Più in generale, l'analisi del dato testuale consente di affermare come il GDPR non risulti richiamato dall'AI Act solamente per ragioni di tecnica normativa, correlate all'esigenza di attingere a definizioni già coniate nell'ambito della disciplina della *data protection* e fatte proprie dal nuovo regolamento.

In argomento, va dato atto non solo della conferma dell'impregiudicata applicabilità del Regolamento generale sulla protezione dei dati, prevista *expressis verbis* dal vigente art. 2, par. 7²², ma anche di ben più rilevanti richiami ad istituti specifici.

19. Parlamento europeo, risoluzione legislativa del 13 marzo 2024 sulla proposta di AI Act.

20. In argomento, tra i vari contributi editi, sovente di carattere introduttivo, si vedano MIOTTO 2023 e CICCIA ROMITO 2021.

21. Si pensi al caso della videosorveglianza intelligente, peraltro contraddistinto da ulteriori elementi di complessità, dovuti alla potenziale rilevanza anche giuslavoristica del tema: cfr. SOFFIENTINI 2023, p. 245 ss.

22. Tale esplicitazione risulta essere stata inserita dagli emendamenti approvati dal Parlamento europeo nel mese di giugno 2023, mediante l'art. 2, par. 5 *bis*, della proposta di regolamento sull'AI, che disponeva quanto segue: «Il diritto dell'Unione in materia di protezione dei dati personali, della vita privata e della riservatezza delle comunicazioni si applica ai trattamenti di dati personali in relazione ai diritti e agli obblighi stabiliti nel presente regolamento. Il presente regolamento lascia impregiudicati i regolamenti (UE) 2016/679 e (UE) 2018/1725

È questo il caso di quanto attiene alla valutazione d'impatto sulla protezione dei dati (o DPIA – *Data Protection Impact Assessment*²³); in materia, oltre al richiamo di cui all'art. 26, par. 9, rivolto ai *deployer* di sistemi di intelligenza artificiale ad alto rischio, rileva anche il successivo art. 27, interamente dedicato alla disciplina di un'altra valutazione d'impatto, quella «sui diritti fondamentali per i sistemi di IA ad alto rischio».

In esso emergono alcuni significativi punti di contatto tra le due discipline, che meritano di essere evidenziati e valorizzati: al par. 4, in particolare, si dispone che, «se uno qualsiasi degli obblighi di cui al presente articolo è già rispettato mediante la valutazione d'impatto sulla protezione dei dati effettuata a norma dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 27 della direttiva (UE) 2016/680, la valutazione d'impatto sui diritti fondamentali di cui al paragrafo 1 integra tale valutazione d'impatto sulla protezione dei dati».

Si tratta, in concreto, di una previsione normativa che mira ad una ottimizzazione degli adempimenti, evidenziando, al contempo, non solo l'imprescindibile coerenza contenutistica tra le due differenti valutazioni, ma anche – e soprattutto – l'opportunità di una valutazione caratterizzata da una più ampia visuale, che sappia cogliere, anche dalla normativa in materia di *data protection*, elementi di potenziale interesse per un'ottimale valutazione – e gestione – dei rischi sui diritti fondamentali.

In merito al rispetto del principio generale di trasparenza previsto dal GDPR, il vigente art. 50, par. 3, contempla per i *deployer* – abbandonando il termine “utenti”²⁴ – «di un sistema di riconoscimento delle emozioni o di un sistema di categorizzazione biometrica», l'obbligo di informazione delle persone fisiche coinvolte «in merito al funzionamento del sistema», anche se non più «in modo tempestivo, chiaro e comprensibile» e senza che venga espressamente richiamato il riferimento al consenso, precedentemente riscontrabile²⁵.

A *latere*, è sempre l'art. 50, par. 3, a confermare – in modo ridondante – l'obbligo, per tali *deployer*, di conformarsi, nel trattare i dati personali mediante siffatti specifici sistemi di intelligenza artificiale, alla normativa eurounitaria in materia di *data protection*.

Più ampiamente, in argomento, risulta meritevole di attenzione l'art. 86 dell'AI Act, rubricato *Diritto alla spiegazione dei singoli processi decisionali*, non presente nella originaria proposta di regolamento ed il cui disposto riproduce, con modificazioni, quello dell'art. 68 *quater*, introdotto nel mese di giugno 2023 ad opera dell'emendamento n. 630. Al par. 1, infatti, si sancisce il diritto di «qualsiasi persona interessata oggetto di una decisione adottata dal deployer sulla base dell'output di un sistema di IA ad alto rischio [...] e che produca effetti giuridici o in modo analogo incida significativamente su tale persona in un modo che essa ritenga avere un impatto negativo sulla sua salute, sulla sua sicurezza o sui suoi diritti fondamentali

e le direttive 2002/58/CE e (UE) 2016/680, fatte salve le disposizioni di cui all'articolo 10, paragrafo 5, e all'articolo 54 del presente regolamento». Si noti come, nell'ultimo testo emendato prima della definitiva approvazione del regolamento, il disposto del paragrafo in questione, rinumerato, risultasse sostanzialmente invariato, eccezion fatta per il rinvio all'art. 59, in luogo dell'art. 54, poi confluito definitivamente nell'art. 2, par. 7, attualmente in vigore.

23. Tale istituto viene richiamato anche dal vigente art. 59, par. 1, lett. c), analogamente a quanto rinvenibile nell'ultimo testo disponibile della proposta di regolamento, mentre, in precedenza, era contemplato dall'art. 54, par. 1, lett. c) della proposta, come modificata dall'emendamento n. 510 approvato a giugno 2023. La norma, ora, riporta riferimenti a «meccanismi di monitoraggio efficaci per individuare eventuali rischi elevati per i diritti e le libertà degli interessati di cui all'articolo 35 del regolamento (UE) 2016/679 e all'articolo 39 del regolamento (UE) 2018/1725 durante la sperimentazione nello spazio di sperimentazione e meccanismi di risposta per attenuare rapidamente tali rischi e, ove necessario, interrompere il trattamento».
24. Come, invece, emergeva nel disposto dell'art. 52, par. 2, anche in esito alla modifica ad opera dell'emendamento n. 485, approvato nel mese di giugno 2023.
25. Non risultano ricomprese nel vigente disposto dell'articolo *de quo* anche queste specificazioni, introdotte sempre ad opera dell'emendamento n. 485, concernenti le modalità di veicolazione delle informazioni e la predeterminazione del consenso dell'interessato quale base giuridica dello specifico trattamento.

[...] di ottenere dal deployer spiegazioni chiare e significative sul ruolo del sistema di IA nella procedura decisionale e sui principali elementi della decisione adottata».

Interessante anche il caso dell'art. 10, par. 5²⁶, ove oggi si stabiliscono le condizioni da osservare obbligatoriamente e congiuntamente al fine di rendere possibile e lecito, seppur in via eccezionale, il trattamento di categorie particolari di dati personali, «nella misura in cui ciò sia strettamente necessario al fine di garantire il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio».

Infine, nel 2023, durante l'iter di approvazione della proposta di regolamento, era stata introdotta nel nuovo punto 4 *bis* dell'allegato IV, ove si enumerano i contenuti della documentazione tecnica prevista nei casi di cui all'art. 11, par. 1, l'obbligatorietà di una «dichiarazione attestante che tale sistema di IA è conforme ai regolamenti (UE) 2016/679 e (UE) 2018/1725 e alla direttiva (UE) 2016/680», nei casi in cui un sistema di AI comporta il trattamento di dati personali²⁷; tale dichiarazione risulta, oggi, ancora espressamente prevista dal vigente AI Act, sebbene attualmente riportata al punto 5 dell'Allegato V, relativo alla dichiarazione di conformità UE.

Ciò posto, pur prescindendo da più o meno significativi richiami testuali, talora riferiti solamente a talune categorie di sistemi di IA, è ben possibile affermare che, ad oggi, non vi possono essere dubbi in relazione all'applicabilità della vigente disciplina eurolunitaria in materia di *data protection* a quei trattamenti che, nell'esercizio di attività d'impresa, già contemplano, anche solo in parte, il ricorso a siffatta tecnologia.

In altre parole, un utilizzo strumentale dell'intelligenza artificiale nel contesto di specifici trattamenti di dati non pare in alcun modo poter escludere l'applicabilità del GDPR, sussistendo gli elementi che determinano l'ambito di applicazione materiale o territoriale di quest'ultimo²⁸ e, comunque, purché si tratti di dati personali, per tali intendendosi, a mente dell'art. 4, par. 1, n. 1), GDPR, informazioni di qualsivoglia natura riguardanti «una persona fisica identificata o identificabile» e, quindi, un «interessato».

Proprio su questo punto, peraltro, si gioca una delle sfide più rilevanti, seppur non tra le più note e adeguatamente attenzionate – tanto nella prassi imprenditoriale, quanto a livello dottrinale – concernente l'anonimizzazione dei dati personali (o, *ab initio*, la natura non personale dei dati medesimi), che reca con sé, quale relevantissimo corollario, l'inapplicabilità della disciplina in materia di *data protection*²⁹.

Posto che, *ex lege*, la natura personale del dato può derivare anche da una mera potenziale ed indiretta identificabilità dell'interessato, l'anonimizzazione, a maggior ragione con particolare riguardo a database particolarmente ricchi ed articolati, non può essere perseguita mediante modalità semplicistiche, quali la mera omissione di nomi e cognomi.

In argomento, il Regolamento generale sulla protezione dei dati personali non pare fornire significativi elementi all'interprete, né contribuire a delineare standard condivisi finalizzati a valutare e gestire il rischio di reidentificazione degli interessati, limitandosi ad operare, al considerando 26, un puntiforme riferimento alla nozione di sufficientemente anonimizzazione di dati personali³⁰.

26. Il paragrafo è stato modificato nel 2023 dall'emendamento n. 290 e, più di recente, nella sopra richiamata risoluzione legislativa del Parlamento europeo del 13 marzo 2024, ad opera della quale sono stati introdotti non solo riferimenti al GDPR, ma anche le condizioni che devono sussistere congiuntamente ai fini della liceità dello specifico trattamento, come definitivamente consacrate nel testo vigente.

27. Così l'emendamento n. 762 alla proposta di regolamento.

28. Cfr. artt. 2 e 3 GDPR.

29. Giova precisare che la non applicabilità del Regolamento generale sulla protezione dei dati non implica una assenza di disciplina specifica, la quale va individuata nel regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

30. Tale nozione può essere maggiormente delineata evidenziando i confini con quella di pseudonimizzazione, alla luce anche della più recente elaborazione giurisprudenziale in materia e, in particolare, della sentenza pronunciata dal Tribunale eurolunitario il 26 aprile 2023, nella causa T-557/20.

Ulteriori e più specifici spunti possono essere tratti dal parere del Gruppo di lavoro articolo 29 n. 5/2014 sulle tecniche di anonimizzazione (WP216)³¹, in particolare per quanto concerne gli aspetti metodologici ed applicativi della randomizzazione e della generalizzazione, intese quali macrocategorie, all'interno delle quali sono individuate plurime tecniche.

Più in generale, l'approccio del WP216 risulta basato su una valutazione ulteriore rispetto a quelle sinora richiamate, avente direttamente ad oggetto il rischio di reidentificazione, in modo non dissimile da quanto emerge dalla recentissima ISO/IEC 27559:2022 (*Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework*), norma tecnica di fondamentale importanza anche per quanto concerne il ricorso ad una nozione piuttosto relativa, quasi personalizzata, di anonimizzazione.

Nel contesto sinora illustrato, perseguire una sufficiente anonimizzazione dei dati personali e mantenere la medesima nel comunicare a terzi o nel diffondere i dataset in questione può risultare una singolare sfida, anche di natura tecnica, in particolare laddove la circolazione stessa dei dati non personali avvenga per finalità eminentemente commerciali, così come – per quanto interessa maggiormente in questa sede – nei casi in cui venga effettuata ai fini dell'apprendimento o dell'applicazione di sistemi di intelligenza artificiale.

Inoltre, tra le tante questioni giuridicamente rilevanti che pone e porrà il ricorso all'intelligenza artificiale, vi è pure quella della trasparenza (o della conoscibilità, secondo la terminologia preferita nella giurisprudenza amministrativa³²), anche in relazione ai profili rilevanti in materia di *data protection*.

Sul punto, prescindendo dai riferimenti espressi attualmente presenti nel testo vigente dell'AI Act, può risultare utile richiamare un recente chiarimento dell'Autorità Garante per la protezione dei dati personali³³.

Si tratta di un "decalogo" che contempla alcune indicazioni per la corretta ed effettiva applicazione

della normativa in materia di protezione dei dati personali, in relazione a quanto pertiene alla «realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale».

La disamina di tale testo consente di trarre alcuni significativi primi spunti, che peraltro paiono in grado di travalicare quanto direttamente concerne l'ambito sanitario: in altri termini, tale elaborazione dell'Autorità Garante per la protezione dei dati personali non solo può agevolare la comprensione delle peculiarità dei trattamenti di dati personali operati tramite strumenti di intelligenza artificiale, ma anche favorire in concreto un'ottimale applicazione della disciplina di cui al GDPR.

Il Garante, anzitutto, riconosce la necessità «che, nella descrizione dei trattamenti, siano puntualmente indicate le logiche algoritmiche utilizzate al fine di "generare" i dati e i servizi attraverso i suddetti sistemi di IA, le metriche utilizzate per addestrare il modello e valutare la qualità del modello di analisi adottato, le verifiche svolte per rilevare la presenza di eventuali bias, le misure correttive eventualmente adottate, le misure idonee a verificare, anche a posteriori, le operazioni eseguite da ciascun soggetto autorizzato e i rischi insiti nelle analisi deterministiche e stocastiche»³⁴.

Nella stessa sede, sempre guardando all'intersezione tra intelligenza artificiale e vigente disciplina in materia di *data protection*, l'Autorità chiarisce in modo ancor più esplicito la cogente imprescindibilità di andare oltre la piena osservanza di quanto sancito *expressis verbis* nel Regolamento generale sulla protezione dei dati, dovendosi informare gli interessati «non solo in merito agli elementi di cui ai richiamati artt. 13 e 14 del Regolamento ma anche evidenziando [...] se il trattamento sia effettuato nella fase di apprendimento dell'algoritmo (sperimentazione e validazione) ovvero nella successiva fase di applicazione dello stesso, nell'ambito dei servizi sanitari, rappresentando le logiche e le caratteristiche di elaborazione dei dati», indicando altresì eventuali specifici obblighi, responsabilità

31. ARTICLE 29 DATA PROTECTION WORKING PARTY 2014.

32. *Ex multis*, cfr. Consiglio di Stato, VI sez., sentenza n. 1206/2021.

33. AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI 2023; il testo, elaborato dall'Autorità nel mese di settembre 2023, è stato pubblicato, in quello successivo, sul sito istituzionale.

34. *Ibidem*.

e benefici correlati all'utilizzo di sistemi di intelligenza artificiale³⁵.

Da tali approdi ermeneutici del Garante sembrano pertanto potersi desumere utili considerazioni che, andando oltre lo specifico ambito cui il “decalogo” intende riferirsi, non possono non interpellare il mondo delle imprese e, segnatamente, quanto concerne l'adeguatezza degli assetti.

3.2. ...alla sicurezza informatica

Non meno rilevanti, inoltre, risultano i profili di *cybersecurity* nell'ambito dell'intelligenza artificiale³⁶, anch'essi pregni di rilevanza giuridica, e che meriterebbero una crescente attenzione e maggiori investimenti, *a fortiori* considerata la perfettibile adozione di presidi tecnico-informatici in ambito societario, in special modo da parte delle PMI.

L'approccio *risk based* – imperniato sul principio di *accountability*, che pervade il GDPR³⁷ e non risulta affatto alieno all'AI Act – contempla anche l'esigenza di non sottovalutare gli ulteriori legami tra sicurezza informatica e trattamento dei dati personali.

Saranno infatti il titolare e l'eventuale responsabile del trattamento a mettere in atto – anche per quei trattamenti che prevedono il ricorso a sistemi di intelligenza artificiale – delle «misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio», determinandone

ex ante l'adeguatezza «tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche»³⁸.

Non solo misure tecnico-informatiche, dunque, ma anche misure organizzative, che tengano conto della singolare rilevanza del “fattore umano” anche nello specifico ambito della sicurezza informatica³⁹ e che possano in modo adeguato prevenire – e gestire – eventuali violazioni dei dati personali.

A tali considerazioni, si aggiunga, pur senza pretese di completezza, il riferimento all'applicabilità – a specifiche realtà societarie – di più stringenti vincoli normativi, principalmente di matrice unionale.

È questo il caso, in particolare, della direttiva (UE) n. 2022/2555 (meglio nota come direttiva NIS 2)⁴⁰, il cui ambito di applicazione, a mente dell'art. 2, par. 1, esula dal novero dei soli soggetti pubblici, ricomprendendo anche gli enti privati «delle tipologie di cui all'allegato I o II»⁴¹ che integrano o superano i requisiti dimensionali propri delle medie imprese e «che prestano i loro servizi o svolgono le loro attività all'interno dell'Unione».

La disciplina della NIS 2 trova altresì applicazione, in talune tassative ipotesi previste *ex lege*, anche in assenza del superamento dei massimali

35. *Ibidem* (corsivo dell'Autore).

36. Anche la rilevanza di tali profili è riconosciuta a livello sovranazionale. Per tutti, sia sufficiente il riferimento a quanto stabilito in OECD 2024. Si tratta della raccomandazione dell'OCSE dedicata all'intelligenza artificiale, adottata il 22 maggio 2019 e recentemente modificata il giorno 8 novembre 2023 e, da ultimo, il 3 maggio 2024 – in cui emergono significativi riferimenti ai principi di *robustness, security and safety*. A tale raccomandazione hanno aderito, tra gli altri, gli Stati Uniti d'America e l'Italia.

37. *Ex multis*, cfr. COLAPIETRO-IANNUZZI 2017, p. 106.

38. A mente dell'art. 32, par. 1, GDPR.

39. *Ex multis*, cfr. SOTIRA 2020 e FANTINI 2008, p. 422.

40. Si tratta della direttiva (UE) n. 2022/2555 del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.

41. Gli allegati I e II enumerano rispettivamente i settori ad alta criticità e “altri settori critici”, ulteriormente articolati in sottosettori e specifici tipi di soggetti. A titolo meramente indicativo, tra i settori contemplati nel primo allegato, figurano energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario ed infrastrutture digitali; nel secondo, invece, sono ricompresi servizi postali e di corriere, fabbricazione, produzione e distribuzione di sostanze chimiche, produzione, trasformazione e distribuzione di alimenti, fornitura di servizi digitali, ricerca.

per le medie imprese di cui alla Raccomandazione 2003/361/CE⁴².

Per quanto maggiormente interessa in questa sede, tra i punti salienti della disciplina, come anticipato applicabile anche a determinate realtà societarie, emerge il capo IV (recante *Misure di gestione del rischio di cibersicurezza e obblighi di segnalazione*) e, in particolare, gli artt. 20 e 21, rubricati rispettivamente *Governance* e *Misure di gestione dei rischi di cibersicurezza*.

In relazione a queste ultime, secondo uno schema non dissimile da quello caratterizzante l'art. 32 GDPR, si prevede che «i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi»⁴³.

4. Alcuni spunti circa l'adeguatezza degli assetti digitali

Le sintetiche considerazioni sinora illustrate – pur senza pretesa di esaustività – mirano a gettare ulteriore luce sui profili problematici, se non di vera e propria criticità, emergenti in ambito societario per quanto concerne la concreta gestione delle tecnologie digitali.

In particolare, prima di evidenziare come il ricorso a sistemi di intelligenza artificiale possa rientrare tra quelli che la dottrina considera “rischi tecnologici d'impresa”⁴⁴, le esemplificazioni proposte evidenziano come la debita presa in considerazione – servendosi funzionalmente di una

opportuna opera ricognitiva – di discipline settoriali e caratterizzate da una significativa portata innovativa non possa prescindere da una visione d'insieme, che – come si è avuto modo sinteticamente di evidenziare – sia in grado di fare emergere anche la rilevanza trasversale di quanto pertiene all'adozione di misure tecniche e organizzative adeguate, così come alla previa valutazione ed alla continua gestione dei rischi.

Sotto quest'ultimo profilo, va altresì apprezzata in concreto la crescente importanza riconosciuta al vigente quadro normativo in materia di *data protection*, come evidenziata dalla recente dottrina che, con gli occhi del giurista, si è interessata all'ambito del *risk management*⁴⁵.

D'altra parte, le nuove sfide poste (anche) dall'intelligenza artificiale invitano l'interprete, già da oggi, a non procedere per compartimenti stagni nella gestione dei rischi, non essendo più sufficiente la mera attribuzione di autonoma dignità e rilevanza ad una specifica disciplina, senza vagliare le confluenze interdisciplinari tra vari ambiti specifici.

Risulta altresì improcrastinabile l'esigenza di un effettivo superamento dell'approccio formalistico talora emergente in sede di *compliance* normativa⁴⁶, sempre più inadatto soprattutto nei contesti ad elevata innovazione tecnologica. Anche in questo caso, interessanti spunti possono essere attinti dall'ambito del *risk management*, laddove scienze giuridiche e aziendalistiche trovano costruttivi e non del tutto esplorati spazi di dialogo e di reciproca fruttuosa influenza.

Se è vero che «la gestione del rischio rappresenta oggi l'architrave di una buona *corporate governance*»⁴⁷ – come peraltro confermato all'interno dei Principi di *Corporate Governance* G20/OCSE

42. Cfr. art. 2, parr. 2, 3 e 4, direttiva NIS 2.

43. Così l'art. 21, par. 1, della direttiva NIS 2, ove si statuisce peraltro che l'adozione di tali misure debba avvenire «tenuto conto delle conoscenze più aggiornate in materia e, se del caso, delle pertinenti norme europee e internazionali, nonché dei costi di attuazione, le misure di cui al primo comma assicurano un livello di sicurezza dei sistemi informatici e di rete adeguato ai rischi esistenti. Nel valutare la proporzionalità di tali misure, si tiene debitamente conto del grado di esposizione del soggetto a rischi, delle dimensioni del soggetto e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico».

44. Si veda, in proposito, SCHNEIDER 2023, pp. 32-33.

45. Cfr. VERONESE 2019, p. 275 ss.

46. In senso sostanzialmente conforme, si rimanda, per tutti, a VERNERO-PARENA-ARTUSI 2019, p. 33.

47. Così MONTALENTI 2019, p. XVII.

di settembre 2023⁴⁸ – tale affermazione può valere, *a fortiori*, nel contesto della *Corptech governance* e, quindi, ai fini di una strutturazione adeguata degli assetti digitali societari.

Il tutto senza dimenticare la rilevanza di quanto sinora affermato all'interno del più ampio contesto degli assetti organizzativi, amministrativi e contabili che, a mente dell'art. 2086, comma 2, c.c., «l'imprenditore, che operi in forma societaria o collettiva, ha il dovere di istituire», avendo peraltro cura che siano in concreto adeguati «alla natura e alle dimensioni dell'impresa»⁴⁹.

Tali assetti, inoltre, vanno considerati non solamente nell'ottica funzionale alla rilevazione tempestiva della crisi d'impresa, come pure attualmente sancito *expressis verbis* nel prosieguo del medesimo art. 2086, comma 2, c.c.⁵⁰, ma quale obbligo di più ampio respiro, intimamente connaturato alla corretta gestione dell'impresa collettiva, in modo non dissimile dalla previsione codicistica di cui all'art. 2381 c.c.⁵¹.

In argomento, risulta imprescindibile sottolineare come l'adozione di sistemi di intelligenza artificiale e, segnatamente, l'inclusione dei medesimi negli assetti organizzativi di una società, travalichi gli obblighi di portata generale, evidenziati nei paragrafi precedenti, comportando invero il necessario riferimento a norme fondamentali del diritto societario.

Sul punto, l'adeguatezza degli assetti, introdotta espressamente a livello codicistico con la riforma del diritto societario del 2003, viene riconosciuta quale «elemento qualificante dei principi di corretta gestione»⁵² e sorta di declinazione dei medesimi⁵³, come emerge anche *ex art.* 2403 c.c., ove viene attribuito dal legislatore al

collegio sindacale il dovere di vigilanza, fra l'altro, «sul rispetto dei principi di corretta amministrazione ed in particolare sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato».

Si tratta di una clausola generale, la cui piena osservanza può in concreto comprimere l'autonomia privata, così come la libertà di iniziativa economica⁵⁴, laddove le scelte dell'organo gestorio devono risultare finalisticamente orientate anche all'adeguatezza degli assetti.

Se, come efficacemente sintetizzato da autorevole dottrina, la predisposizione – e successiva gestione – di adeguati assetti può essere considerata come «il dovere organizzativo di più elevato grado»⁵⁵, il ricorso a sistemi di intelligenza artificiale, che pure implica una idonea proceduralizzazione, contribuisce a far emergere ulteriormente la crescente ed «accentuata complessità e rischiosità delle scelte manageriali»⁵⁶.

Ciò posto, nel considerare le implicazioni del ricorso a sistemi di intelligenza artificiale in ambito societario, risulta necessario riconoscere l'imprescindibilità, prima ancora di una corretta gestione dei «rischi tecnologici in senso stretto», ontologicamente correlati ad una specifica tecnologia, di quel «rischio prevalentemente strategico» che si radica ogniqualvolta quest'ultima venga introdotta nel contesto dell'esercizio di attività d'impresa⁵⁷.

5. Il ruolo della *Corporate Digital Responsibility*

Emerge quindi come un approccio orientato al *risk management* – più precisamente, alla gestione integrata del rischio propria dell'*Enterprise Risk*

48. Cfr. OECD 2023. Si noti come, all'interno di tale documento, venga auspicata, a supporto dell'organo gestorio, la costituzione di gruppi di esperti, secondo criteri di flessibilità e proporzionalità alle esigenze specifiche.

49. Per tutti, in argomento, si veda CAVALIERE 2019, p. 1943 ss.

50. Cfr. PANZANI 2020, p. 656.

51. *Ex multis*, cfr. BRUNO 2020, p. 51.

52. Così MONTALENTI 2016, p. 6.

53. *Ex multis*, cfr. IRRERA 2005, p. 69.

54. Cfr. MERUZZI 2016, pp. 43-44 e 53-54.

55. IRRERA 2005, p. 81.

56. NAPPO 2020, p. 90.

57. SCHNEIDER 2023, p. 32.

*Management*⁵⁸ –, corroborato da una corretta e non parcellizzata visione e gestione delle varie tecnologie digitali utilizzate in una specifica realtà societaria, possa far sì che non vadano perduti frammenti giuridicamente rilevanti anche ai fini dell'osservanza del principio generale di corretta amministrazione.

In altre parole, ciò potrebbe massimizzare anche i benefici che possono derivare da un ricorso al digitale che non sia solo formalmente *compliant*, ma anche sostanziale ed efficiente applicazione di quelle regole di condotta che l'organo gestorio dovrà sempre più tenere in considerazione – sebbene caratterizzate da una formulazione generica o, talora, priva di natura cogente – nelle loro concrete declinazioni.

Ampliare lo sguardo, considerare il rischio come un *upside risk*, foriero anche di opportunità, adottare procedure interne che, partendo da una mappatura delle tecnologie e dalla definizione dei ruoli, possano concretamente incidere nella predisposizione di assetti digitali adeguati, soprattutto di natura organizzativa, costituiscono condotte non solo utili, ma anche doverose nel contesto dell'ordinario esercizio di attività d'impresa.

Le molteplici peculiarità dell'intelligenza artificiale giuridicamente rilevanti in ambito societario, considerate *una cum* i recenti approcci del *risk management*, come evidenziati dalla più autorevole dottrina, possono altresì suggerire di attenzionare l'ambito della *Corporate Digital Responsibility* che, in argomento, può giocare un ruolo molto rilevante.

Essa è stata tratteggiata anzitutto come una “sottocategoria” della *Corporate Social Responsibility* nei primi recepimenti ad opera della dottrina italiana, che ne ha evidenziato il legame con l'ambito tecnologico che maggiormente interessa in questa sede e, in particolare, ai «coessenziali profili di responsabilità digitale di quelle società che includono nei propri assetti tecnologie di intelligenza

artificiale»⁵⁹. Elementi di responsabilità sociale d'impresa vengono altresì evocati con particolare riguardo alla correttezza della strutturazione e dell'utilizzo delle “tecnologie societarie”, peraltro «avendo attento riguardo ai possibili impatti sociali e ambientali delle stesse»⁶⁰.

Ciò posto, risulta opportuno non circoscrivere in via esclusiva l'ambito di pertinenza della *Corporate Digital Responsibility* ad una determinata tecnologia, onde evitare di vanificare quei benefici di singolare rilevanza informatico-giuridica che possono derivare significativamente solo da un qualificato sguardo d'insieme relativo agli assetti digitali di una determinata realtà societaria.

Inoltre, ulteriori approcci dottrinali confermano che la *Corporate Digital Responsibility*, seppur caratterizzata da significative affinità con quanto pertiene alla sostenibilità sociale, sia caratterizzata da una autonoma rilevanza⁶¹: in argomento, la dottrina tedesca si è spinta a considerare quanto concerne il ricorso agli strumenti digitali, nel contesto dell'esercizio di attività d'impresa, un vero e proprio settore della *Corporate Responsibility*⁶².

Tali considerazioni circa la crescente opportunità di sposare un inquadramento tassonomico della *Corporate Digital Responsibility* che sia in grado di evidenziarne l'autonoma rilevanza e, al contempo, di coglierne i profili dinamici⁶³, intendono costituire uno stimolo ad ulteriori studi in materia, nella consapevolezza che la responsabilità digitale d'impresa rappresenta uno stimolante crogiolo, punto d'incontro tra le competenze interdisciplinari degli esperti e le esigenze degli amministratori, in grado di favorire la migliore gestione delle multiformi sfide del digitale in ambito societario, con riguardo anche all'adozione di sistemi di intelligenza artificiale.

In argomento, l'apporto del giurista informatico può giocare un ruolo determinante nel coadiuvare

58. Un approccio integrato (e interdisciplinare) specificamente riferito ai rischi dell'intelligenza artificiale si riscontra nell'*Integrated AI-Risk Management* (IARM), «processo aziendale di risk management autonomo [...] sia pure sempre inserito in quello più generale di gestione del rischio d'impresa» proposto e descritto in CERRATO-CULASSO-CROCCO 2023, p. 319 ss.

59. SCHNEIDER 2022, p. 720.

60. *Ibidem*.

61. A titolo esemplificativo, si veda LOBSCHAT-MUELLER-EGGERS et al. 2021, p. 876.

62. DÖRR 2021, pp. XIII e 2.

63. *Ivi*, pp. 5 e 35 ss.

l'approfondimento concernente i rischi tecnologici d'impresa, stimolando un'analisi del rapporto tra diritto societario e tecnologie digitali improntata ad un approccio olistico e che sia in grado, al contempo, di far tesoro dei rilevanti spunti desumibili dai più recenti approdi della dottrina.

Riferimenti bibliografici

- N. ABRIANI, G. SCHNEIDER (2021), *Diritto delle imprese e intelligenza artificiale. Dalla Fintech alla Corp-tech*, il Mulino, 2021
- ARTICLE 29 DATA PROTECTION WORKING PARTY (2014), *Opinion 05/2014 on Anonymisation Techniques*, 2014
- AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (2023), *Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale*, 2023
- M. BIANCHINI, G. GASPARRI, G. RESTA et al. (a cura di) (2022), *Gli sviluppi tecnologici del diritto societario*, Quaderni giuridici CONSOB, n. 23, 2022
- R. BORRUSO, S. RUSSO, C. TIBERI (2009), *L'informatica per il giurista. Dal bit a Internet*, Giuffrè, 2009
- S. BRUNO (2020), *Cambiamento climatico e organizzazione delle società di capitali a seguito del nuovo testo dell'art. 2086 c.c.*, in "Banca, Impresa, Società", 2020, n. 1
- T. CAVALIERE (2019), *Codice della crisi d'impresa e dell'insolvenza. Le modificazioni del Codice civile*, in "Giurisprudenza Italiana", 2019, n. 8-9
- S.A. CERRATO, F. CULASSO, E. CROCCO (2023), "Handle with care". Per una governance dell'intelligenza artificiale nell'impresa: rischi, tecniche di gestione, assetti cibernetici, in N. Abriani e R. Costi (a cura di), "Diritto societario, digitalizzazione e intelligenza artificiale. In ricordo di Agostino Gambino", Giuffrè, 2023
- S.A. CERRATO (a cura di) (2019), *Impresa e rischio. Profili giuridici del risk management*, Giappichelli, 2019
- C. CICCIA ROMITO (2021), *Il GDPR nella micro, piccola e media impresa*, Giuffrè, 2021
- R.M. COLANGELO (2023), *Informatica giuridica e impresa: nuove prospettive di Corporate Digital Responsibility*, in "Rivista elettronica di Diritto, Economia, Management", 2023, n. 2
- C. COLAPIETRO, A. IANNUZZI (2017), *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. Califano e C. Colapietro (a cura di), "Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679", Editoriale Scientifica, 2017
- S. DÖRR (2021), *Corporate Digital Responsibility. Managing Corporate Responsibility and Sustainability in the Digital Age*, Springer Verlag, 2021
- L. ENRIQUES, D.A. ZETZSCHE (2019), *Corporate Technologies and the Tech Nirvana Fallacy*, ECGI, Law Working Paper n. 457/2019
- EUROPEAN COMMISSION (2023-A), *Report on the state of the Digital Decade 2023*, 2023
- EUROPEAN COMMISSION (2023-B), *Report on the state of the Digital Decade 2023. Annex Italy*, 2023
- M. FANTINI (2008), *Phishing: strategie operative dell'inganno*, in "Diritto dell'Internet", 2008, n. 4
- M. IRRERA (2005), *Assetti organizzativi adeguati e governo delle società di capitali*, Giuffrè, 2005
- ISTAT (2023), *Rilevazione sulle tecnologie dell'informazione e della comunicazione (Ict)*, 2023
- P. LIBERANOME (2022), *Criptoarte e nuove sfide alla tutela dei diritti autorali*, in "I Contratti", 2022, n. 1
- L. LOBSCHAT, B. MUELLER, F. EGGERS et al. (2021), *Corporate digital responsibility*, in "Journal of Business Research", 2021, n. 122

- D. MATRICANO (2020), *Fare impresa nell'era digitale. Analisi teoriche e riflessioni critiche su un processo business-driven e technology-enabled*, Giappichelli, 2020
- A. MICOZZI (a cura di) (2024), *L'attivazione imprenditoriale in Italia. Rapporto GEM 2023-2024*, FrancoAngeli, 2024
- L. MIOTTO (2023), *Organizzazione d'impresa e gestione dei dati personali. Il rischio di non compliance nelle catene di fornitura*, Giappichelli, 2023
- P. MONTALENTI (2019), *Introduzione*, in S.A. Cerrato (a cura di), "Impresa e rischio. Profili giuridici del risk management", Giappichelli, 2019
- P. MONTALENTI (2016), *I principi di corretta amministrazione*, in M. Irrera (a cura di), "Assetti adeguati e modelli organizzativi nella corporate governance delle società di capitali", Zanichelli, 2016
- G.D. MOSCO (2019), *Roboboard. L'intelligenza artificiale nei consigli di amministrazione*, in "Analisi Giuridica dell'Economia", 2019, n. 1
- F. NAPPO (2020), *Aziende e intelligenza artificiale. Prime riflessioni critiche*, FrancoAngeli, 2020
- OECD (2024), *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, 2024
- OECD (2023), *G20/OECD Principles of Corporate Governance 2023*, OECD Publishing, 2023
- L. PANZANI (2020), *La disciplina degli assetti ai fini della rilevazione della crisi, con particolare riferimento alla s.r.l.*, in M. Irrera (a cura di), "La società a responsabilità limitata: un modello transtipico alla prova del Codice della Crisi. Studi in onore di Oreste Cagnasso", Giappichelli, 2020
- F. PASCUCCI (2017), *Lo stato della "trasformazione digitale" nelle PMI italiane e sfide emergenti*, in F. Pascucci, V. Temperini (a cura di), "Trasformazione digitale e sviluppo delle PMI. Approcci strategici e strumenti operativi", Giappichelli, 2017
- M. PIETRANGELO (2007), *La società dell'informazione tra realtà e norma*, Giuffrè, 2007
- R. ROLLI (2018), *Il Diritto privato nella società 4.0*, Wolters Kluwer - Cedam, 2018
- G. SCARCHILLO (2019), *Corporate Governance e Intelligenza Artificiale*, in "La nuova giurisprudenza civile commentata", 2019, n. 4
- G. SCHNEIDER (2023), *La proposta di Regolamento sull'intelligenza artificiale: le possibili ripercussioni sull'attività di impresa*, in M. Rescigno (a cura di), "L'impresa nell'era dell'intelligenza artificiale: un'evoluzione tranquilla o nulla sarà più lo stesso?", Giuffrè, 2023
- G. SCHNEIDER (2022), *Intelligenza artificiale, governance societaria e responsabilità sociale d'impresa: rischi e opportunità. Prima parte*, in "La nuova giurisprudenza civile commentata", 2022, n. 3
- M. SOFFIENTINI (2023), *I sistemi di videosorveglianza intelligenti*, in M. Soffientini (a cura di), "Gli adempimenti privacy per i sistemi di videosorveglianza", Giuffrè, 2023
- N. SOTIRA (a cura di) (2020), *Il fattore umano nella cyber security. Valori e strategie da costruire insieme*, FrancoAngeli, 2020
- UNIONCAMERE – ANPAL (2023), *Sistema Informativo Excelsior (2023), Nuove imprese. Caratteristiche e fabbisogni professionali delle nuove imprese. Indagine 2023*, 2023
- P. VERNERO, B. PARENA, M.F. ARTUSI (2019), *Risk management e modelli organizzativi*, in S.A. Cerrato (a cura di) "Impresa e rischio. Profili giuridici del risk management", Giappichelli, 2019
- B. VERONESE (2019), *Privacy 4.0: oneri e strategie per le PMI*, in S.A. Cerrato (a cura di) "Impresa e rischio. Profili giuridici del risk management", Giappichelli, 2019



MATTEO LONGO

Missing Trader Ontology (MTO): un'ontologia per il rilevamento delle società cartiere e la prevenzione delle frodi all'IVA intracomunitaria

Lo sviluppo dei fenomeni fraudolenti in danno dell'IVA intracomunitaria e, in particolare, l'evoluzione delle *Missing Trader Intra-Community VAT fraud* (frodi all'IVA intracomunitaria con utilizzo di società cosiddette "cartiere") obbliga costantemente le Istituzioni Unionali a potenziare ed adeguare le azioni di contrasto, sempre più a carattere preventivo. Le contromisure adottate dagli Stati membri dell'Unione Europea sono risultate spesso disomogenee e non sempre efficaci, anche in ragione delle "tecniche" utilizzate dalle organizzazioni criminali e della rapidità di realizzazione delle frodi. Nell'epoca segnata dal predominio dell'Intelligenza Artificiale, un valido supporto nella lotta alle frodi può essere fornito dall'adozione di un approccio ontologico che, in determinati contesti, conserva dei vantaggi rispetto all'approccio neurale. Lo sviluppo di ontologie applicative, oltre a dotare gli Organi di controllo di una definizione unitaria del fenomeno fraudolento, fornisce l'elemento processabile dagli strumenti di ragionamento automatico per il rilevamento delle società "cartiere" e la prevenzione delle frodi all'IVA intracomunitaria.

Frodi IVA intracomunitaria – Intelligenza Artificiale – Ontologia – Rilevamento – Prevenzione

Missing Trader Ontology (MTO): an ontology for missing trader detection and Intra-Community VAT fraud prevention

The increase in Intra-Community VAT frauds and, mostly, the development of fraudulent phenomena related to Missing Trader Intra-Community VAT frauds constantly pushed European Institutions to strengthen and to adapt enforcement actions, more preventive than in the past. The countermeasures adopted by EU States are often inconsistent and not properly effective, also because of the "techniques" used by criminal organizations and the celerity with which frauds are carried out. In the Artificial Intelligence era, a valid aid in the fight against frauds can be provided by the ontological approach which, in certain application domains, retains advantages over the neural approach. The development of application ontologies, as well as providing a unified definition of the fraudulent phenomenon, provides an element that can be processed by automatic *reasoners* for the *missing trader* detection and the MTIC VAT fraud prevention.

Intra-Community VAT fraud – Artificial Intelligence – Ontology – Detection – Prevention

L'Autore è dottore in Ingegneria informatica e ispettore della Guardia di Finanza. Il presente contributo è espressione solo del pensiero dell'Autore e non coinvolge né impegna in alcun modo l'Amministrazione di appartenenza

SOMMARIO: 1. Introduzione. – 1.1. *Il Mercato unico europeo e le frodi all'IVA intracomunitaria.* – 1.2. *I dati unionali e nazionali sulle frodi IVA.* – 1.3. *La necessità di un approccio unitario, preventivo, risk-analysis-based.* – 2. *MTIC VAT fraud e missing trader: definizione e caratteristiche.* – 2.1. *I tratti distintivi delle MTIC VAT fraud.* – 2.2. *Le caratteristiche e le anomalie della "società cartiera".* – 3. *Le ragioni della scelta dello strumento ontologico.* – 3.1. *I vantaggi dell'approccio ontologico rispetto a un approccio neurale.* – 4. *Costruzione dell'ontologia del missing trader.* – 4.1. *Ontologie nel dominio delle frodi IVA e "stato dell'arte".* – 4.2. *Progettazione dell'ontologia.* – 4.3. *Gli strumenti utilizzati nella costruzione dell'ontologia.* – 4.4. *Le classi dell'ontologia del missing trader.* – 4.5. *Descrizione semantica delle classi.* – 4.6. *Le relazioni nell'ontologia del missing trader.* – 4.7. *Restrizioni sulle proprietà di MTO.* – 4.8. *Creazione dell'entità MissingTrader.* – 4.9. *Requisiti per l'individuazione di un missing trader.* – 5. *Risultati.* – 5.1. *Validazione dell'ontologia.* – 5.2. *Rilevamento del missing trader con uno strumento di ragionamento automatico.* – 5.3. *Discussione dei risultati.* – 6. *Conclusioni.* – 6.1. *Propositi e sviluppi futuri.* – Tabelle.

1. Introduzione

1.1. Il Mercato unico europeo e le frodi all'IVA intracomunitaria

L'istituzione del Mercato unico per gli Stati membri dell'Unione europea, avvenuta il 1° gennaio 1993¹, ha costituito una pietra miliare nel processo di armonizzazione dei principi tecnici e delle norme che regolano la circolazione di merci, servizi, capitali e persone nell'UE.

All'eliminazione dei controlli alle frontiere tra Paesi membri, per quanto attiene all'IVA applicata sugli scambi commerciali realizzati entro i confini dell'Unione, è seguita l'adozione del cosiddetto *principio di destinazione*, in deroga all'ordinario *principio d'origine*.

Il principio di destinazione prevede che un'operazione commerciale di compravendita tra soggetti residenti in differenti Stati membri dell'UE, non sia imponibile ai fini IVA nel Paese di origine del bene/servizio² e che venga invece assoggettata

a imposta nel Paese di destinazione, dove il bene/servizio viene consumato/utilizzato, secondo l'aliquota ivi stabilita. Ciò si sostanzia nella possibilità, riconosciuta al soggetto passivo IVA cedente, di effettuare una cessione intracomunitaria di beni/servizi traslando l'obbligo di assoggettamento ad imposta dell'operazione commerciale sul cessionario, qualora anch'esso sia qualificabile come soggetto passivo IVA.

La traslazione dell'obbligo di adempiere al versamento dell'IVA in capo al cessionario, nell'ipotesi in cui quest'ultimo risulti infedele, può determinare il cosiddetto "salto d'imposta" ovvero il mancato assolvimento dell'IVA in una determinata fase della catena di transazioni commerciali.

L'abuso di tale regime transitorio ha portato alla realizzazione di vari tipi di fenomeni fraudolenti in danno dell'IVA, tra i quali rivestono un ruolo di primaria importanza le frodi internazionalmente riconosciute con il nome di *Missing Trader Intra-Community (MTIC) VAT fraud* o "frodi all'IVA intracomunitaria dell'operatore mancante".

1. L'Atto Unico Europeo, entrato in vigore il 1° luglio 1987, stabiliva una deadline per la realizzazione del mercato interno europeo al 31/12/1992, secondo i propositi definiti nei Trattati di Roma del 1957: «uno spazio senza frontiere interne nel quale è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali». Cfr. Parlamento europeo 2023.

2. Cfr. art. 41 del d.l. 30 agosto 1993, n. 331.

Caratteristica comune alle predette frodi è il coinvolgimento di *missing trader* – “operatori mancanti” o “società cartiere” – soggetti giuridici sovente facenti capo a cosiddetti “prestanome”, solitamente privi di dotazione patrimoniale e organizzazione adeguate all’esercizio di un’attività d’impresa, appositamente costituiti allo scopo di produrre documenti commerciali e fiscali fittizi, attestanti transazioni meramente “cartolari”, atte a consentire di eludere il versamento dell’IVA.

Tali società il più delle volte non presentano alcuna dichiarazione fiscale ed hanno la funzione di “convogliare” sulla propria posizione il debito IVA derivante dalle transazioni commerciali realizzate, per poi far perdere le proprie tracce (da cui l’appellativo di “operatore mancante”) senza versare quanto dovuto all’erario.

Le frodi fiscali portate a termine con il ricorso a *missing trader* costituiscono la forma più diffusa e pericolosa di frode IVA, tanto da meritare un trattamento riservato nei programmi unionali e nazionali di contrasto alla criminalità organizzata. Si tratta infatti di frodi organizzate e messe a punto da gruppi criminali, hanno portata internazionale e sono particolarmente difficili da rivelare in tempi utili ad evitarne il compimento.

1.2. I dati unionali e nazionali sulle frodi IVA

Negli anni «la frode IVA è diventata un’industria consolidata»³, capace di evolversi per adattarsi al contesto giuridico-economico.

L’attacco criminale e organizzato al sistema IVA⁴ non causa solo un ammanco alle finanze unionali ma altera la leale concorrenza dei mercati, in quanto il mancato pagamento dell’IVA a monte permette agli evasori di praticare prezzi di mercato più competitivi, oltre a gettare le basi per la

perpetrazione di ulteriori attività illecite; si ritiene infatti che «i profitti derivanti dalle frodi carosello potrebbero diventare la più importante fonte di finanziamento di altre attività criminali»⁵.

Nel 2018 le “frodi carosello”, le più ricorrenti tra le *MTIC VAT fraud*, sono state definite dal Parlamento Europeo come le frodi all’IVA intracomunitaria più dannose, con perdite di imposta stimate in 50 miliardi di Euro all’anno⁶; dato confermato anche dalle statistiche della Commissione Europea⁷ che per il 2018 hanno visto posizionarsi proprio l’Italia in testa alla classifica dei Paesi europei in relazione al *gap IVA*⁸ stimato, ammontante a circa 35,4 miliardi di Euro; primato conservato anche negli anni 2019 (circa 31,1 miliardi di Euro) e 2020 (circa 26,2 miliardi di Euro)⁹.

Sempre nel 2020 l’UE ha mancato di incassare 99 miliardi di euro di IVA, cifra che avrebbe permesso di finanziare la costruzione di 185 ospedali all’avanguardia o 1.700 chilometri di linee per l’alta velocità ferroviaria (approssimativamente la distanza tra Berlino e Bucarest)¹⁰.

Nel 2021, ultima annualità relativamente alla quale risultano pubblicati i dati inerenti al *VAT gap* stimato, l’IVA evasa a livello europeo ha sfiorato i 61 miliardi di euro, con l’Italia sempre in testa alla classifica dei Paesi europei con la maggiore perdita di imposta (circa 14,6 miliardi di euro)¹¹, sebbene in netto calo rispetto agli anni precedenti, a testimonianza della bontà delle azioni di governo e dell’efficacia degli sforzi profusi in particolar modo da Guardia di Finanza, Agenzia delle Entrate ed Agenzia delle Dogane e dei Monopoli.

Dal gennaio 2017 al maggio 2018, oltre il venticinque per cento dell’IVA evasa e scoperta dalla Guardia di Finanza è risultata connessa a frodi di tipo “carosello”¹², mentre nel triennio 2020-2022

3. International VAT Association 2007.

4. ANDREW-BAER 2023.

5. BORSELLI 2008.

6. LAMENSCH-CECI 2018.

7. EUROPEAN COMMISSION 2020.

8. Per *gap IVA* o *VAT gap* si intende la stima della differenza tra le entrate IVA “attese”, che si sarebbero dovute incassare, e quanta IVA è stata effettivamente riscossa in un determinato arco temporale di riferimento.

9. MOBILI 2022.

10. EUROPEAN COMMISSION 2022.

11. European Commission 2023.

12. TOSCHI 2018.

l'azione sinergica di Guardia di Finanza, Agenzia delle Entrate ed Agenzia delle Dogane e dei Monopoli, ha consentito di individuare e bloccare 260 frodi carosello, per un totale di fatture per operazioni inesistenti emesse pari a oltre 2,2 miliardi di Euro¹³.

1.3. La necessità di un approccio unitario, preventivo, *risk-analysis-based*

Le numerose azioni di contrasto progressivamente poste in essere dagli Stati membri UE, sia individualmente che a livello unionale, hanno arrestato ed invertito il *trend* negativo che vedeva l'ammontare dell'IVA evasa incrementarsi di anno in anno.

L'emanazione della Direttiva UE 2017/1371 (c.d. Direttiva "PIF"), il potenziamento degli strumenti di cooperazione internazionale¹⁴, la creazione di Organismi europei¹⁵ atti a ricercare, perseguire e giudicare fatti lesivi del bilancio e degli interessi dell'UE, la costante attenzione rivolta alle *MTIC VAT fraud* con la promozione di progettualità come EMPACT 2022¹⁶ sono infatti alcuni dei provvedimenti adottati in ambito comunitario e che indirizzano l'azione dei singoli Paesi membri.

Parallelamente, l'estensione del regime di inversione contabile (c.d. *reverse charge*) a diversi settori commerciali considerati a rischio frodi IVA, l'introduzione dello *split payment* e della fatturazione elettronica (di cui l'Italia può considerarsi l'"apripista" in Europa), unitamente all'inasprimento delle sanzioni di carattere penale (introdotto con D.L. n. 124/2019 e D.L. n. 75/2020, in recepimento della c.d. "Direttiva PIF") e all'adozione di specifici piani operativi antifrode da parte della Guardia di

Finanza, sono alcune delle principali contromisure poste in essere a livello nazionale che hanno contribuito a conseguire risultati incoraggianti.

Tuttavia la battaglia alle frodi IVA è ancora lontana dall'essere vinta e alle misure di contrasto prospettate dall'Unione Europea non sempre è seguita un'appropriate risposta da parte dei singoli Stati membri.

Se è vero che ogni Stato può far valere i propri obblighi impositivi anche nei confronti di soggetti passivi non residenti, è altrettanto vero che il raggio d'azione degli ordinari strumenti di ricerca e soppressione dei fenomeni evasivi è limitato entro i confini del territorio nazionale.

Per far fronte a tali criticità, con la Direttiva 2010/24/UE e il Regolamento 904/2010 del Consiglio dell'Unione Europea è stata introdotta una serie di strumenti atti a favorire la mutua assistenza tra gli Stati membri in materia di recupero dei crediti fiscali e di scambio di informazioni per il rintraccio degli evasori e la riscossione dell'imposta evasa. Tuttavia, per quanto riguarda la cooperazione tra i Paesi UE, la Corte dei Conti Europea ha sentenziato che le strutture amministrative e le procedure operative poste in essere dai singoli Stati sono inadeguate, le risposte alle richieste di informazioni inoltrate dai loro omologhi pervengono spesso in ritardo, incomplete e non sempre vengono utilizzate¹⁷.

I controlli e le strategie messe in atto dai diversi Stati, inoltre, hanno livelli qualitativi e di avanguardia tecnologica sensibilmente differenti: finché taluni Stati membri utilizzano strumenti e tecnologie maggiormente all'avanguardia rispetto

13. MINISTERO DELL'ECONOMIA E DELLE FINANZE 2022.

14. Ne sono esempi lo scambio spontaneo o su richiesta di informazioni tra Stati membri, l'alimentazione di banche dati a carattere internazionale come VIES – Vat Information Exchange System o ancora l'adesione volontaria a progetti quali EUROCANET – European Carousel Network.

15. Quali EUROJUST (Agenzia dell'Unione Europea per la cooperazione giudiziaria penale), EUROFISC (una rete di cooperazione amministrativa tra Stati in ambito IVA), OLAF (Ufficio Europeo per la lotta antifrode) ed EPPO (Procura Europea con sede in Lussemburgo, composta da procuratori provenienti da ogni Stato dell'UE partecipante).

16. Progetto che tra le priorità per il periodo 2022-2025 cita il proposito di «ostacolare la capacità delle reti criminali e degli imprenditori individuali criminali coinvolti in frodi all'IVA intracomunitaria con utilizzo di *missing trader*». Cfr. EUROPOL 2022.

17. CORTE DEI CONTI EUROPEA 2008.

ad altri, «i truffatori possono concentrarsi sui “porti più deboli”»¹⁸.

Per garantire una maggiore impermeabilità ai fenomeni criminali è importante tenere a mente che le frodi intracomunitarie, in quanto tali, «non possono essere combattute efficacemente con un approccio nazionale»¹⁹, per cui «un obiettivo più complesso ma essenziale consiste nella creazione di un sistema di “analisi di rischio” a livello UE, il quale avrebbe un effetto sinergico dato dall'intreccio delle esperienze maturate dai singoli Stati membri»²⁰.

La Corte dei conti olandese (*Algemene Rekenkamer*), l'omologa Suprema Istituzione federale di controllo tedesca (*Bundesrechnungshof*) e la Corte dei conti belga (*Rekenhof*), congiuntamente, hanno fornito delle “raccomandazioni” circa gli accorgimenti che sarebbe opportuno adottare per prevenire la commissione delle frodi all'IVA intracomunitaria²¹:

- valutare preventivamente le richieste di attribuzione dei numeri identificativi IVA;
- potenziare il sistema informativo di supporto per la segnalazione dei rischi e prioritizzare la gestione dei segnali di allarme: «il supporto di un sistema informativo è necessario per generare segnali di allarme (selezione dei rischi) e a far fronte alle restrizioni temporali (una valutazione manuale non è attuabile). Le tecniche di estrazione dei dati/profilazione dei rischi possono tornare utili allo scopo.»;
- fare uso delle informazioni sugli autori di precedenti reati nella valutazione dei rischi: sebbene essere a conoscenza del passato “criminale” di un soggetto non possa determinare un divieto all'esercizio di una sua attività economica, può costituire un'informazione utile nel processo di valutazione dei rischi;
- prestare maggiore attenzione ai rischi legati al trasferimento della proprietà di quote societarie: «L'esperienza maturata nel campo delle

frodi IVA dimostra che il trasferimento di quote societarie nasconde dei rischi. I potenziali truffatori possono tentare di utilizzare società già esistenti (acquisendone quote di partecipazione al capitale sociale, ndr.) evitando le procedure di registrazione (di nuove società, ndr.).».

Sul punto è intervenuto anche il Legislatore nazionale, emanando da ultima la Legge n. 197/2022²² (Legge di Bilancio 2023), al cui articolo 1, comma 148, ha incaricato l'Agenzia delle Entrate²³ di applicare nuove misure preventive per il contrasto dei fenomeni evasivi legati principalmente al rilascio delle «nuove partite IVA», alle società «caratterizzate da brevi cicli di vita o da ridotti periodi di operatività», alle imprese già operanti che «dopo un periodo di inattività o a seguito di modifiche dell'oggetto o della struttura, riprendono ad operare», mancando di adempiere agli obblighi dichiarativi e fiscali.

Tali misure si sostanzierebbero in «specifiche analisi del rischio connesso al rilascio e all'operatività delle partite IVA, al fine di individuare tempestivamente i soggetti che presentano criticità o anomalie», «anche sulla base dei dati trasmessi e degli esiti delle istruttorie della Guardia di Finanza»²⁴.

In tal senso un'importante impulso allo sviluppo di strumenti atti a rilevare i fenomeni evasivi e capaci di condurre una *data-driven risk analysis* (analisi dei rischi basata su dati) è stato dato dalla Commissione Europea, la quale ha dato il via libera al finanziamento del progetto dell'Agenzia delle Entrate “*A data driven approach to tax evasion risk analysis in Italy*”, che prevede l'applicazione dell'intelligenza artificiale e in particolare delle tecniche di *network analysis*, *machine learning* e *data visualization* «al fine di realizzare un nuovo sistema di supporto ai processi di individuazione dei soggetti ad alto rischio di frodi fiscali»²⁵.

18. BORSELLI 2008.

19. *Ibidem*.

20. *Ibidem*.

21. ALGEMENE REKENKAMER-BUNDESRECHNUNGSHOF-REKENHOF 2009.

22. Cfr. art. 35, co. 15-bis.1 e 15-bis.2 del d.P.R. 26 ottobre 1972, n. 633.

23. Cfr. Provvedimento n. 156803/2023 del 16 maggio 2023, a firma del Direttore dell'Agenzia delle Entrate.

24. DIRETTORE DELL'AGENZIA DELLE ENTRATE 2023.

25. AGENZIA DELLE ENTRATE 2021.

È quantomai auspicabile, dunque, l'adozione di un approccio unitario a carattere preventivo che, ancor prima di “rincorrere” i frodatori, li individui nelle fasi iniziali di preparazione della frode o quantomeno ne rilevi i tratti caratteristici e le anomalie grazie alle quali sarebbe possibile svelare il progetto criminale.

Il presente lavoro, incardinandosi nell'ambito delle opportunità offerte dalle moderne tecnologie, propone uno strumento basato su una forma precursora di Intelligenza Artificiale, capace di rilevare automaticamente la presenza di una “società cartiera” e di fornire supporto alle tradizionali tecniche di indagine impiegate nella lotta alle frodi IVA dell'operatore mancante.

2. MTIC VAT fraud e missing trader: definizione e caratteristiche

2.1. I tratti distintivi delle MTIC VAT fraud

Le difficoltà nel farne emergere l'impianto frodatario risiedono principalmente nella rapidità e nell'utilizzo di differenti modalità di esecuzione, quindi nel coinvolgimento di numerosi soggetti economici che, articolando e ramificando la catena di transazioni realizzate, offuscano il quadro entro cui si trovano ad operare gli investigatori e gli addetti alla vigilanza fiscale.

L'organizzazione delle frodi in argomento prevede la definizione di precisi ruoli, rivestiti di volta in volta dai soggetti coinvolti, i quali consentono di tracciare uno schema e di ricondurlo all'una o all'altra tipologia di frode.

Nel suo schema “base”, una MTIC VAT fraud si realizza quando un soggetto stabilito in un determinato Stato membro (anche detto *conduit*

*company*²⁶) rifornisce un secondo soggetto stabilito in un diverso Paese UE, il cosiddetto *missing trader*, tipicamente una società “fittizia” non esercitante alcuna attività economica lecita. Quest'ultimo cede ad un utilizzatore, a prezzi estremamente vantaggiosi, i beni precedentemente acquisiti, forte del mancato assolvimento degli obblighi IVA²⁷. Il terzo soggetto, nella catena di transazioni appena descritta, può talvolta agire da *broker* e trasferire nuovamente la proprietà dei beni in un diverso Stato membro ad un altro *missing trader* o ad un'altra *conduit company* dando vita a quella che è conosciuta come “frode carosello”.

La reiterabilità e l'integrabilità, potenzialmente illimitate, di un siffatto schema di frode fanno sì che da esso possano scaturirne ulteriori, più complessi e meno agevoli da individuare all'aumentare dei soggetti, degli Stati e delle transazioni coinvolte.

Oltre all'onnipresente *missing trader* e alla *conduit company*, altre figure tipicamente riscontrabili in presenza di MTIC VAT fraud, sono quelle del *buffer*²⁸ e del già citato *broker*²⁹.

I principali schemi di frode all'IVA intracomunitaria con utilizzo di società cartiere sono invece riconducibili convenzionalmente alle già menzionate “frodi di acquisizione” e “frodi carosello”, cui si aggiungono le cosiddette *Missing Trader Intra-Community fraud - Cross-Invoicer*, che contengono e combinano entrambe le precedenti, e le *Missing Trader Intra-Community fraud - Contra-trading* che abbinano una catena di transazioni legittima alla catena fraudolenta, avvalendosi di un *contra-broker*, figura di raccordo tra le due catene di transazioni.

Ogni schema nell'elenco appena stilato – a partire da quello meno articolato, tipico della MTIC *Acquisition fraud* – può quindi essere considerato

26. Con il termine *conduit company* si indica la società residente in uno Stato membro diverso da quello in cui risiede il *missing trader*, la quale ha il compito di effettuare transazioni con esso, dando origine alle frodi intracomunitarie.

27. Lo schema di frode descritto prende il nome di “frode di acquisizione” o *Missing Trader Intra-Community Acquisition fraud*.

28. Per *buffer* si intende un operatore commerciale apparentemente “ordinario”, “connazionale” della società cartiera, che acquista beni o servizi dalla stessa per rivenderli ad altri soggetti appartenenti all'organizzazione criminale; appositamente interposto per dare una parvenza di regolarità alla catena di transazioni commerciali e rendere più difficoltosa la rivelazione della macchina fraudolenta.

29. Il termine *broker* nel contesto di riferimento sta ad indicare un soggetto economico, residente nel medesimo Stato membro di appartenenza del *missing trader* o del *buffer*, che acquista beni o servizi da questi ultimi per poi rivenderli al consumatore finale o ad altro soggetto passivo IVA, facendo ripartire il “carosello”.

un'evoluzione di quello che lo precede, appositamente arricchito di soggetti, transazioni e condotte lecite o illecite atte ad ostacolarne l'individuazione e a celarne le reali finalità³⁰.

Tale elenco di schemi fraudolenti non può tuttavia ritenersi esaustivo giacché, come anticipato, la semplice interposizione di ulteriori agenti consentirebbe di derivare, potenzialmente, innumerevoli altri.

Il rimando ai sopra elencati “*cliché*”, inoltre, può senz'altro essere utile ad avere un riferimento cui raffrontarsi nel processo di rilevamento di eventuali frodi ma, in considerazione della loro integrabilità, non è particolarmente importante l'analisi delle componenti del singolo schema, quanto l'estrazione delle caratteristiche affini alla macro-categoria di frodi in argomento.

Ponendosi in un rapporto gerarchico di generalizzazione/specializzazione, qualsiasi schema fraudolento – *sottoclasse* della *classe* delle *MTIC VAT fraud* – ne eredita le caratteristiche peculiari, utili a risalire alla *classe genitore*.

I tratti distintivi generali, comuni a tutti gli *esemplari* della *classe* delle *MTIC VAT fraud*, risiedono principalmente:

- nella realizzazione di operazioni commerciali intracomunitarie, ovvero poste in essere tra soggetti residenti in diversi Stati membri UE, senza le quali, banalmente, non sarebbe perseguibile lo scopo della sottrazione illecita dell'I-Va intracomunitaria;
- nei settori commerciali e merceologici in cui si instaurano dette frodi: i beni più frequentemente oggetto delle transazioni fraudolente sono (storicamente) le autovetture, i beni tecnologici, i metalli preziosi, i prodotti petroliferi ed in generale tutti quei beni altamente diffusi tra la popolazione mondiale e connotati da alto costo unitario e facilità di trasporto, proprietà che consentono di commercializzarne grandi

volumi in estese aree geografiche. Negli ultimi anni le frodi hanno avuto ad oggetto anche beni intangibili come servizi inerenti alle telecomunicazioni, *carbon credits* e certificazioni di “energia green”;

- nella scelta di commercializzare beni e servizi solitamente offerti conseguendo ridotti margini di guadagno, per i quali la fissazione di prezzi di vendita particolarmente competitivi può assicurare in poco tempo l'acquisizione di consistenti quote di mercato e lo sbaraglio della concorrenza;
- nella preferenza per le categorie di merci la cui cessione è assoggettata ad aliquota IVA ordinaria (solitamente la più elevata), per comprensibili ragioni di efficienza del sistema fraudolento.

Il concetto fondante e imprescindibile, da cui prende il nome la classe di frodi in argomento, è comunque costituito dal *missing trader*.

L'istituzione e l'utilizzo di una società “cartiera”, artefice materiale del salto d'imposta, costituisce il grimaldello attraverso il quale viene scardinato il sistema IVA.

La centralità di tale entità, d'altro canto, rappresenta anche il punto focale del problema dalla prospettiva delle autorità fiscali, poiché individuando l'“operatore mancante” in una fase propedeutica al compimento della frode o, preferibilmente, in fase di attribuzione della partita IVA o di autorizzazione all'effettuazione di operazioni intracomunitarie³¹, si può impedire che una frode venga organizzata e portata a termine: «l'“analisi dei rischi” preventiva è diventata elemento essenziale di contrasto alle frodi»³².

2.2. Le caratteristiche e le anomalie della “società cartiera”

Il *missing trader* è un'entità – solitamente costituita in forma di società di capitali, prevalentemente a responsabilità limitata o semplificata – priva di

30. Per approfondimenti sugli schemi di frode con utilizzo di “società cartiere” più diffusamente rilevati si rimanda a EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR TAXATION AND CUSTOMS UNION 2018.

31. L'attribuzione della partita IVA è necessaria per ogni operatore che intende esercitare un'attività economica nel territorio dello Stato; l'analogo codice identificativo valido in ambito europeo prende il nome di *VAT identification number*. L'autorizzazione all'effettuazione delle operazioni intracomunitarie, invece, richiede l'inserimento dell'operatore che ne fa richiesta nell'archivio VIES (*VAT Information Exchange System*), il quale raccoglie i dati dei soggetti autorizzati a compiere operazioni commerciali intracomunitarie e i flussi degli scambi intercorsi tra i soggetti stessi.

32. BORSELLI 2008.

organizzazione, consistenza economica e dotazione patrimoniale tali da consentirle l'esercizio di un'attività d'impresa. Usualmente stabilita in Paesi caratterizzati da ordinamenti giuridici particolarmente flessibili e poco orientati a rigidi controlli, la "società cartiera" è tipicamente inoperativa, poiché di recente costituzione o più datata ma inattiva, e connotata da breve "vita". Non di rado si tratta di società create *ad hoc* per fruirne relativamente a un numero limitato di operazioni, spesso nell'ambito del compimento di una sola frode, che si estinguono dopo periodi di tempo relativamente brevi, dell'ordine di pochi mesi o anni.

Gli amministratori di detti "operatori mancanti" sono abitualmente soggetti indigenti, inoccupati, irreperibili o domiciliati all'estero, privi di conoscenze specifiche del settore in cui opera la società cui sono posti a capo, a volte addirittura ignari di esserne i "gestori".

I soggetti realmente controllanti tali imprese risultano invece spesso gravati da precedenti specifici, sono criminali associati in organizzazioni diffuse in ambito nazionale o comunitario, i veri promotori delle frodi.

Una definizione autorevole di "società cartiera" è ravvisabile in quella che il Gruppo d'Azione Finanziaria Internazionale – GAFI (internazionalmente riconosciuto come FATF – *Financial Action Task Force*) definisce *shell company*, ovvero una società di comodo, principalmente a responsabilità limitata o in forma simile, che con l'uso di amministratori e azionisti "prestanome", in rapporto di dipendenza da altri soggetti, frapponendo uno "schermo" tra questi ultimi (i reali beneficiari del compimento della frode) e i proventi illeciti, ponendo in essere operazioni meramente cartolari, essendo sprovvista di mezzi umani e materiali idonei a svolgere un'attività economica³³.

Un profilo ugualmente rilevante della "società cartiera" è stato tracciato dalle numerose sentenze emesse dalla Corte di Cassazione³⁴, le quali ne descrivono le caratteristiche peculiari:

- forma giuridica a responsabilità limitata o comunque semplificata;
- presenza di amministratori e legali rappresentanti c.d. "teste di legno";

- assenza di struttura organizzativa, personale dipendente e dotazione patrimoniale;
- assenza di bilanci depositati;
- mancata sottoscrizione, totale o parziale, di dichiarazioni fiscali;
- "operatività" in settori principalmente riconducibili al commercio di autovetture, beni tecnologici, carburanti e ai servizi di consulenza professionale, trasporti e logistica;
- presenza di ingenti flussi finanziari in entrata seguiti da cospicui flussi in uscita su rapporti finanziari esteri;
- esecuzione di operazioni finanziarie "circolari", ovvero somme di denaro dapprima incassate ed in seguito retrocesse ai rispettivi "finanziatori".

L'UIF – Unità di Informazione finanziaria per l'Italia ha stilato un corposo elenco di anomalie/criticità che contraddistinguono le "società cartiere"³⁵, afferenti al profilo soggettivo e oggettivo di tali entità, relative a concetti attinenti al dominio amministrativo/finanziario. Gli elementi di anomalia/criticità in parte riutilizzati per la definizione di *missing trader* che verrà illustrata nel seguito, saranno presentati nel corso della trattazione dedicata alla costruzione del "modello" del *missing trader* stesso.

Occorre da subito precisare, invece, che ai fini dell'individuazione di un potenziale *missing trader* non è necessario che siano presenti tutti gli elementi distintivi esposti; parimenti la concorrente presenza di più caratteristiche/anomalie in relazione ad un determinato soggetto non può ritenersi sufficiente per la definizione di una "società cartiera".

Le peculiarità sin qui riportate costituiscono riferimenti autorevoli e qualificati per la valutazione del rischio legato all'operatività di determinate economie, elaborati da Autorità ed Organismi nazionali e internazionali, che per la loro applicazione a casi concreti richiedono un'accorta valutazione e la considerazione del contesto operativo da cui originano.

La definizione "per analogia" offerta dal GAFI, ad esempio, nasce dai riscontri effettuati nell'ambito della sorveglianza attiva anti-riciclaggio; le sentenze emanate dalla Suprema Corte possono

33. FATF/GAFI 2018.

34. Liberamente consultabili sul [portale](#), utilizzando le parole chiave "cartiera" o "*missing trader*" per le ricerche.

35. PELLEGRINI-DE FRANCESCHIS-BENTIVOGLI-LAURENZA 2020.

invece essere riconducibili a contesti molto differenti; il profilo soggettivo e oggettivo tracciato dall'UIF, infine, fa riferimento a dati e informazioni estraibili da vari database o dall'esame di vicende societarie e bilanci d'esercizio.

Ai fini del presente lavoro, tali constatazioni impongono di effettuare una selezione delle caratteristiche e degli elementi di criticità più confacenti al caso di studio, attinente alla valutazione dei tratti identificativi di potenziali "società cartiere" in una fase prodromica alla realizzazione di una frode IVA "dell'operatore mancante".

Prevenire il compimento di una frode si traduce nella necessità di un intervento tempestivo quando la stessa si trova ancora in uno stadio "embrionale", quando non sono ancora state messe a punto le condotte tipiche per la realizzazione dell'azione criminale.

Il requisito della tempestività mal si confà a tutte quelle anomalie che possono essere rilevate in seguito all'analisi di copiosa documentazione societaria e contabile, dall'esame di flussi e movimenti finanziari, dalla consultazione di banche dati alimentate con cadenza periodica (come *VIES*), incompatibili con le tempistiche di realizzazione di una frode all'IVA intracomunitaria.

Il bisogno di ricevere *alert* preventivi, che mettano in guardia gli operatori del settore, rimandando ad un secondo momento l'approfondimento e le valutazioni del caso, può essere soddisfatto dalla realizzazione di un sistema di valutazione del rischio basato su un'*ontologia* della "società cartiera", strumento che può risultare di ausilio non solo ad Autorità, Enti ed Organizzazioni, ma anche ad operatori economici e privati, sia su base territoriale che su scala nazionale o internazionale.

3. Le ragioni della scelta dello strumento ontologico

La semplice disponibilità di dati, seppure in grandissima quantità e di certa qualità/affidabilità, non implica la padronanza dell'informazione in essi contenuta, per l'estrazione della quale, in ogni circostanza, è richiesto un processo di elaborazione dei dati che può essere anche molto complesso e dispendioso in termini di tempo e risorse impiegate.

La smisurata quantità di informazione non strutturata – a causa della mancanza di aggregazione e qualificazione dei dati – disponibile su

un'architettura decentralizzata, autonoma e paritetica com'è gran parte del Web conosciuto oggi, in cui ogni utente è libero di organizzare ed esporre contenuti senza badare ad accordi di significato, determina la dispersione delle risorse, complicandone il reperimento, la comprensione e l'elaborazione per l'estrazione di informazione.

I risultati delle ricerche in rete sono dati che derivano da fonti eterogenee, spesso espressi in formati "non aperti", inadeguati semanticamente poiché forniti in linguaggio naturale che è connotato da polisemia, omonimia, sinonimia, vaghezza, tutti limiti ineliminabili poiché insiti nel linguaggio naturale stesso.

La non corretta indicizzazione dei contenuti, inoltre, li rende irrintracciabili e a volte sostituiti da risultati che possono risultare non pertinenti con l'oggetto della ricerca.

I dati, in conclusione, hanno bisogno di una componente soggettiva, data dall'interpretazione dell'agente, e di essere interconnessi tra loro per fornire compiutamente informazione. Basti pensare a quante parole e simboli possono assumere significati differenti, in base alla percezione dell'interprete e al contesto in cui sono immersi.

I processi cognitivi che portano l'uomo a interpretare un simbolo e ad attribuirgli un significato, nonché a porlo in rapporti di interrelazione con altri concetti, sono frutto di esperienza, sensibilità e di una componente intellettuale data dall'intuito, dall'abilità naturale di *inter-lègere*, di andare oltre la mera rappresentazione simbolica; componenti cognitive estranee ai comuni "cervelli elettronici" e non (ancora) integralmente rimpiazzabili da forme di Intelligenza Artificiale.

L'esigenza di velocizzare ed automatizzare un processo di ricerca, di estrarre informazione coerente e di elaborarla logicamente per legarla ad altri concetti propri del dominio d'interesse, necessita che le macchine deputate allo svolgimento di questi compiti abbiano accesso a collezioni di dati strutturati e messi in relazione tra loro (*Linked Data*), oltre a regole di inferenza logica sui dati che, subentrando alla componente intellettuale umana, siano capaci di effettuare ragionamenti automatici e dedurre conoscenza "nuova" da conoscenze pregresse.

La realizzazione di un simile sistema informativo, frutto della composizione di un sistema informatico e della componente umana,

passa necessariamente per la «ricerca di un sistema comune e condiviso per la comunicazione e comprensione dell'informazione»³⁶.

Al fine di garantire una corretta ed efficiente interazione tra l'operatore umano ed un sistema software si rende quindi necessario definire un *vocabolario condiviso* che permetta di descrivere il significato dei concetti appartenenti ad un dominio d'interesse, secondo una semantica che sia non ambigua ed elaborabile da una macchina. «Descrivere questa semantica, cioè quello che normalmente viene chiamato significato inteso dei termini di un vocabolario è il compito delle *ontologie* per il Semantic Web»³⁷.

Secondo una celebre definizione di Thomas Gruber un'ontologia è una «specificazione formale ed esplicita di una concettualizzazione condivisa»³⁸: «specificazione» sta ad indicare una dichiarazione, l'esplicitazione di un concetto; l'essere «formale» ed «esplicita» attiene alla modalità con cui il concetto deve essere espresso, cioè in modo che sia comprensibile e processabile da una macchina; una «concettualizzazione» è una rappresentazione astratta, un modello di un concetto in un dominio d'interesse, «condivisa» perché l'ontologia rappresenta la conoscenza universalmente riconosciuta e consensualmente accettata da una comunità.

Una concezione elaborata da Robert Neches (e altri), maggiormente orientata agli aspetti pratico-realizzativi di un'ontologia, la definisce come «l'insieme dei termini basilari e delle relazioni che costituiscono il vocabolario di una specifica area e delle regole per combinare termini e relazioni per estendere il vocabolario»³⁹.

Un'ontologia, quindi, è dotata di una dimensione dinamica e in evoluzione, legata alla generazione di nuovi termini e nuove relazioni, deducibili da quelli posti a fondamento dell'ontologia stessa.

Le necessità, cui si è già accennato, di:

- rappresentare formalmente il contenuto di un concetto e dotarlo di un significato comune;
- mettere in correlazione logica diversi concetti per derivare nuove informazioni e rappresentare fattispecie complesse;

- far convergere i vari Enti e le varie Organizzazioni a livello europeo sul *significato inteso* di *missing trader*;
 - agevolare la cooperazione tra Autorità appartenenti ai diversi Stati membri;
 - realizzare l'interoperabilità semantica tra i servizi già esistenti;
 - favorire l'interazione uomo-macchina per l'identificazione di tali entità in contesti a rischio di complesse frodi all'IVA intracomunitaria;
 - offrire un contributo per lo sviluppo di agenti software capaci di processare le informazioni contenute nell'ontologia per dedurre nuove conoscenze su diversi domini d'interesse,
- risultano soddisfatte, per definizione, dall'ontologia.

3.1. I vantaggi dell'approccio ontologico rispetto a un approccio neurale

Un sistema *ontology-based* si presta ad integrazioni e sviluppi, è capace di evolvere insieme ai fenomeni fraudolenti e alle tecnologie in uso, si rende fruibile per differenti categorie di utilizzatori (utenti comuni ed operatori esperti), favorisce il confronto tra ordinamenti giuridici diversi garantendo una base tecnologica comune ed agevolando l'adozione di misure di contrasto uniformi.

Sebbene la scelta dell'approccio ontologico possa apparire «fuori moda» in un momento storico in cui spadroneggia l'approccio neurale e il *deep learning*, il contesto di riferimento non appare propriamente adatto all'elaborazione di reti neurali o all'applicazione di modelli «LLM» (*Large Language Model*) per una serie di motivi.

Le informazioni da processare, attinte nel dominio delle frodi IVA, sono spesso basate su dati che, presi singolarmente, non sono fortemente rappresentativi di alcuna circostanza e che mutano con il contesto socio-economico di riferimento o al variare delle tecniche utilizzate per compiere le frodi. Necessitando di interrelazioni con altre evidenze per l'estrazione di informazione, tali dati si prestano ad essere processati in maniera più efficace da parte di strumenti ontologici piuttosto

36. OLTRAMARI-BORGIO-CATENACCI et al. 2003.

37. *Ibidem*.

38. GRUBER 1993.

39. NECHES-FIKES-FININ et al. 1991.

che neurali, i quali, tra l'altro, sono più soggetti all'*overfitting*.

Come sarà chiarito nel seguito, l'ontologia qui definita affonda le radici su (relativamente) pochi concetti fondamentali, dati dalle caratteristiche peculiarmente riscontrabili in presenza di *missing trader*, per la cui valutazione non sono richieste particolari elaborazioni.

Una volta definito un vocabolario di termini basilari, dopo aver identificato quali relazioni intercorrono tra detti termini e aver definito delle regole per la combinazione di termini e relazioni, si può ricavare una "traduzione" formale del concetto che si intende rappresentare, in termini informatici, aderente al dominio di appartenenza e ai requisiti prescelti.

Gli approcci neurali, al contrario, richiedono una grande quantità di dati per il loro *addestramento* e la definizione di numerosi parametri per garantire l'affidabilità delle risposte che andranno a fornire.

L'indisponibilità di rilevanti moli di dati strutturati, derivanti da casi concreti e qualitativamente accettabili, sia a causa della frammentarietà delle informazioni conoscibili sia per ragioni legate alla privacy dei soggetti coinvolti, costituisce un ostacolo per lo sviluppo di sistemi basati sul *deep learning*.

Il fattore temporale che dipende proporzionalmente dalla difficoltà di reperimento ed elaborazione delle informazioni rappresenta un altro problema di cui tenere conto.

I modelli neurali, inoltre, sono connotati da una certa *opacità*, dovuta alla loro complessità e alla difficoltà nell'interpretazione della loro struttura; non è sempre agevole comprenderne i ragionamenti che poi danno origine alle decisioni restituite e, di conseguenza, intervenire per risolvere eventuali difetti.

Il disegno di legge sull'Intelligenza Artificiale, in attesa di specifiche norme che adeguino l'ordinamento nazionale al regolamento europeo conosciuto come "*AI Act*", approvato lo scorso 20 maggio in Senato con l'obiettivo, tra gli altri, di promuovere un utilizzo *trasparente* dell'intelligenza

artificiale, pone in evidenza proprio le criticità legate alla trasparenza dei *meccanismi* coinvolti nell'elaborazione delle decisioni e degli algoritmi che conducono alle stesse, trasparenza che si rende necessaria sia al fine di rendere partecipi i soggetti interessati dei criteri su cui si basano tali decisioni, sia a dimostrarne sufficientemente la fondatezza e la legittimità qualora tali decisioni vengano adottate anche dall'operatore umano che le ha richieste.

Le ontologie, diversamente dai modelli neurali, sono *trasparenti*, facilmente intelleggibili ed adattabili, conferiscono chiarezza e comprensibilità ai concetti e alle relazioni che rappresentano, consentendo un più proficuo utilizzo di un limitato numero di dati e la riusabilità degli stessi in contesti differenti; tale aspetto facilita anche l'interoperabilità tra sistemi diversi e la condivisione di conoscenza.

4. Costruzione dell'ontologia del *missing trader*

4.1. Ontologie nel dominio delle frodi IVA e "stato dell'arte"

L'elaborazione di ontologie per la realizzazione di sistemi atti a rilevare frodi non costituisce una novità in termini assoluti nel panorama informatico mondiale, tuttavia, con riferimento ad eventuali ontologie afferenti al dominio delle frodi all'IVA, non esistono contributi prontamente (ri)utilizzabili.

Le *MTIC VAT fraud* sono legate alle "falle" del sistema IVA, le quali indubbiamente differiscono dalle fragilità che potrebbero affliggere sistemi di imposizione indiretta extra-unionali.

L'esame delle pubblicazioni aventi ad oggetto lo studio di approcci ontologici al problema delle frodi IVA ha comunque evidenziato la prevalenza di riferimenti a frodi finanziarie in senso lato⁴⁰ oppure a tipologie di frodi ben definite ma non rientranti nella categoria delle frodi all'IVA⁴¹.

Altri contributi si avvicinano al problema delle frodi IVA da un punto di vista giuridico-legale ed offrono spunti per la realizzazione di strumenti

40. Cfr. ALEXOPOULOS-KAFENTZIS-BENETOU et al. 2007.

41. Cfr. HUSSAINI-GUESSOUM-MERCIER-LAURENT 2022; TANG-LIU-YANG-WEI 2018; ATTIGERI-PAI-RADHIKA PAI-KULKARNI 2018; FANG-CAI-FU-DONG 2007.

*ontology-based*⁴² ma non modellano semanticamente il concetto di frode IVA o di *missing trader*.

Termini afferenti al dominio d'interesse sono definiti dall'ontologia AMLO-core (*Anti Money Laundering Ontology core*)⁴³, specificamente realizzata per la rappresentazione della conoscenza in ambito anti-riciclaggio. Tuttavia, la stretta attinenza ad un settore differente da quello delle frodi IVA ed il suo essere "derivata" in larga parte dal set di ontologie FIBO (*Financial Industry Business Ontology*)⁴⁴ – i cui concetti non risultano completamente definiti, totalmente differenziati e comunque non interamente "discendenti" da ontologie *top-level* – ne scoraggiano il riutilizzo.

Ad ogni modo, per la realizzazione dell'ontologia della società "cartiera" si è ritenuto opportuno attingere e far derivare i concetti necessari direttamente da ontologie "fondamentali", tra tutte DUL (*DOLCE+DnS Ultralite*)⁴⁵, evitando così di importare definizioni che, seppur idealmente accettabili, sono frutto dell'adattamento ad uno specifico ambiente applicativo.

Tracce di interessanti studi teorici in materia di ontologie e frodi IVA riconducono al FF POIROT⁴⁶ Consortium che nell'ambito dell'omonima progettualità finanziata dalla Commissione Europea, tra il 2002 e il 2005 ha condotto un'analisi sugli aspetti legali e giuridici legati al potenziale impiego di un modello ontologico per l'individuazione di frodi IVA. Le conclusioni tratte dagli studiosi nell'ambito del sopracitato progetto, in cui si rispecchiano i propositi su cui si basa il presente lavoro, avvalorano l'approccio ontologico poiché «una migliore comprensione dei fattori di rischio connessi alle frodi potrebbe portare a un migliore orientamento dei controlli e a un rafforzamento significativo della prevenzione delle frodi»⁴⁷, dove per "fattori di rischio" si intendono gli elementi che delineano «i profili tipici dei truffatori o delle transazioni fraudolente

che indirizzano gli investigatori verso la fase iniziale di possibili frodi»⁴⁸.

4.2. Progettazione dell'ontologia

La progettazione dell'ontologia della "società cartiera" – *Missing Trader Ontology* (nel seguito più semplicemente *MTO*) – come si è già accennato, ha avuto origine dall'individuazione degli elementi di criticità e di anomalia caratterizzanti tale "tipologia" di società, distinguibili sulla base dell'appartenenza al *profilo soggettivo* o al *profilo oggettivo* del soggetto giuridico.

Oltre al profilo operativo (*oggettivo*) che indubbiamente pone in risalto condotte rilevanti, le "società cartiere" condividono tratti comuni attinenti ad un profilo più marcatamente *soggettivo*, delineato dalle caratteristiche proprie del soggetto giuridico considerato. Gli elementi identificativi di carattere soggettivo sopperiscono alla difficoltà di "tracciamento" delle operazioni economiche e societarie realizzate dal presunto *missing trader*, offrendo al contempo dati immediatamente riscontrabili, legati alla "fisionomia" dell'entità esaminata; l'esame delle condotte e delle vicende societarie potrebbe richiedere invece tempi tecnici più estesi e il ricorso a metodologie d'analisi meno immediate.

Una volta definito il *dominio d'interesse*, evidentemente riconducibile al settore delle frodi all'IVA intracomunitaria, l'approccio progettuale adottato è stato di tipo *middle-out*: la selezione degli elementi di anomalia/criticità e la loro definizione ha fornito implicitamente una serie di *concetti*, rappresentabili in *classi* su cui basare l'ontologia.

I concetti così definiti sono stati oggetto di elaborazioni aventi "direzioni" opposte: sono state operate *generalizzazioni* per collegarli a *super-classi* di entità sovraordinate, inerenti a ontologie con livello più alto di astrazione, e sono state effettuate operazioni di *specializzazione* per raffinare i

42. BUKHSH-WEIGAND 2015.

43. Modulo "principale" dei progetti AMLO, relativi alla rappresentazione di fatti e informazioni legati al settore dell'anti-riciclaggio.

44. Insieme di *ontologie* rappresentanti il dominio delle imprese finanziarie.

45. Ontologia consultabile sul sito del CNR-ISTC.

46. Acronimo di *Financial Fraud Prevention Oriented Information Resources Using Ontology Technology*.

47. VANDENBERGHE-SCHAFER-KINGSTON 2003.

48. *Ibidem*.

concetti ed “estrarne” di ulteriori, da ricondurre a *sotto-classi* di entità contraddistinte da minore astrazione e maggiore specificità.

Sebbene la rappresentazione ontologica della “società cartiera” che verrà presentata rientri tra le *application ontology*, ovvero tra le ontologie specifiche di un particolare aspetto del dominio d’interesse e utili a fornire conoscenza per lo sviluppo di applicativi, data l’assenza di ontologie di dominio prontamente integrabili e stante la generalità di taluni aspetti descritti, peculiari delle frodi IVA “dell’operatore mancante” ma comuni ad altre tipologie di azioni criminose, tale ontologia potrebbe costituire una prima approssimazione di *domain ontology* per il dominio delle frodi IVA in senso lato.

Come già anticipato e come verrà più compiutamente illustrato nel seguito, per la modellazione di alcuni concetti fondamentali dell’ontologia si è scelto di “farli discendere” da alcune classi di un’ontologia “fondante”, la già citata *DUL*. Tale scelta è giustificata sia da ragioni di natura logica e di consistenza – in quanto per definire formalmente concetti rappresentanti entità giuridiche, informazioni astratte, ruoli, proprietà, si rende necessario fare ricorso a concetti generali come quelli offerti dalle ontologie “più ad alto livello” (quali *DUL*, ontologia *top-level*) – sia da esigenze di modificabilità, riusabilità e scalabilità, al fine di garantirne la futura integrazione conservando formalità e potenza descrittiva (*target* più difficilmente raggiungibili utilizzando classi e relazioni estratte da ontologie attinenti a uno specifico ambito di riferimento).

Per la denominazione delle classi, delle relazioni e delle loro proprietà, come anche per le descrizioni, le regole e le annotazioni, si è scelto di adottare la lingua inglese per ovvi motivi pratici e di fruibilità, essendo inerenti a tematiche afferenti a un contesto internazionale.

Per la denominazione delle classi si è fatto ricorso alla notazione *CamelBack* con la prima lettera in maiuscolo, mentre per la denominazione delle relazioni e delle istanze la medesima notazione è stata adottata mantenendo la prima lettera in carattere minuscolo, fatta eccezione per le parole composte il cui primo termine è una sigla

(ad esempio, come si vedrà a breve, “*VAT_Id*” – il numero identificativo ai fini IVA).

4.3. Gli strumenti utilizzati nella costruzione dell’ontologia

Per la realizzazione del progetto è stato utilizzato il software open-source *Protégé*⁴⁹ nella versione 5.6.3, il quale offre un ambiente per lo sviluppo di ontologie sia da remoto che on-line⁵⁰.

L’ambiente di sviluppo è dotato di interfaccia grafica *user-friendly* e consente di creare, modificare ed esportare ontologie in linguaggio OWL con sintassi *RDF/XML*, *OWL/XML*, *Turtle* o *Manchester/OWL*.

Protégé è altresì fornito di *reasoner Pellet* per la deduzione di nuova conoscenza da informazioni già acquisite e rappresentate nell’ontologia.

Nella sezione dedicata alla realizzazione dell’ontologia saranno illustrati i passaggi principali relativi all’implementazione del modello semantico in argomento, anche per mezzo di *screenshot* tratti dall’interfaccia grafica del programma.

OWL (*Ontology Web Language*) è un linguaggio basato su logiche descrittive, introdotto dal W3C (*World Wide Web Consortium*, organizzazione internazionale che si prefigge l’obiettivo di favorire lo sviluppo e l’accessibilità del World Wide Web) ed ormai da anni divenuto uno standard per la costruzione di ontologie. Per la realizzazione di questo progetto si è fatto ricorso a OWL 2, l’estensione di OWL attualmente in distribuzione, avente grado di espressività più elevato rispetto alla precedente.

Il prodotto dell’elaborazione tramite software *Protégé* è un documento OWL 2 con sintassi *RDF/XML*, definita dal W3C come “sintassi di scambio primaria” per il linguaggio in oggetto.

RDF (*Resource Description Framework*) offre un modello basato su XML per descrivere e condividere una risorsa ed è lo strumento introdotto dal W3C per l’aggiunta di informazioni descrittive alla risorsa stessa, basate su metadati (definite *statement* o *asserzioni* o *dichiarazioni*), senza necessità di introdurle all’interno come avviene con i *linguaggi di markup* quali HTML e XML.

Un’asserzione in RDF assume la forma “Soggetto – Predicato – Oggetto” ed è comunemente

49. MUSEN 2015.

50. Piattaforma raggiungibile sul sito della [Stanford University](http://stanford.edu).

rappresentata da un grafo orientato: il soggetto è una risorsa di cui si intende “predicare”, ovvero specificare una proprietà, e costituisce il nodo da cui parte l'arco orientato; quest'ultimo rappresenta il predicato, il quale esprime una proprietà o una relazione relativa alla risorsa di partenza; infine l'oggetto, nodo di destinazione del predicato, rappresenta un valore, o un'altra risorsa, legata al soggetto per mezzo del predicato.

Risorse, proprietà e valori definiti da uno *statement* rappresentano, unitamente a quest'ultimo, gli elementi costituenti il modello RDF.

La più volte richiamata DUL (*DOLCE+DnS Ultralite*) è un'ontologia ad alto livello che fornisce una semplificazione dell'ontologia *DOLCE Lite-Plus* e la contestuale integrazione di questa con l'ontologia *Description and Situations* (DnS).

Offre una descrizione di concetti estremamente generali, quindi agevolmente riutilizzabili ed adattabili a domini e contesti eterogenei. La codifica in linguaggio OWL ne ha favorito la diffusione e l'adozione in qualità di ontologia *fondazionale* per innumerevoli progetti.

I concetti più astrattamente formalizzati nell'ontologia del *missing trader* sono stati derivati dalle rispettive concettualizzazioni offerte da DUL. Tali derivazioni saranno puntualmente illustrate nella sezione relativa alla realizzazione di MTO.

4.4. Le classi dell'ontologia del *missing trader*

Gli elementi di criticità relativi al profilo soggettivo ed oggettivo dell' “operatore mancante” costituiscono il punto di partenza nella costruzione dell'ontologia.

Ogni elemento di criticità è stato incapsulato in un concetto e rappresentato da una *classe* (un modello dotato di proprietà che gli individui appartenenti alla classe rispettano).

La classe del *missing trader* è stata formalizzata come sotto-classe del generico “soggetto giuridico” per motivi di *ereditarietà* ed *estensione* della super-classe, nonché per ragioni legate alla validazione dell'ontologia stessa.

Di seguito vengono elencati i concetti, che rispecchiano le anomalie selezionate,

distinguendoli in base all'appartenenza all'uno o all'altro profilo:

– Profilo soggettivo:

1. partita IVA o numero identificativo ai fini IVA inesistente o cessato o associato a un differente soggetto giuridico;
2. «forme giuridiche caratterizzate da flessibilità e semplicità, sia per gli adempimenti previsti in fase costitutiva che sotto il profilo strutturale o gestionale»⁵¹: «la società per azioni è tipicamente la forma giuridica di imprese con una struttura produttiva, un'organizzazione e una governance complessa e stabile, connotati assenti nelle cartiere»⁵²; le forme giuridiche più ricorrenti per le società cartiere sono quelle cosiddette “semplificate”;
3. sede legale, sede amministrativa o luogo di esercizio dell'attività soggetti a cambi frequenti e repentini;
4. «sede legale in un luogo distante da quello in cui risulta essere ubicato il centro degli interessi e/o la sede direzionale»⁵³;
5. oggetto sociale ampio ed estremamente variegato;
6. indisponibilità di uffici, magazzini, sedi locali necessarie per l'esercizio delle attività economiche di cui all'oggetto sociale;
7. inconsistenza o mancato versamento (totale o parziale) del capitale sociale;
8. cariche amministrative e/o di rappresentanza rivestite da soggetti molto giovani o, al contrario, molto anziani: gli amministratori o rappresentanti legali delle società cartiere sono spesso soggetti molto anziani o molto giovani, più facilmente circuibili dai *dominus* della frode;
9. cariche amministrative e/o di rappresentanza rivestite da soggetti estranei al settore commerciale/produttivo in cui opera la società;
10. amministratori e/o rappresentanti legali e/o proprietari di quote societarie soggetti a cambi frequenti o repentini;
11. amministratori e/o rappresentanti legali già ricoprenti le medesime cariche in società inadempienti o liquidate;

51. UIF 2020.

52. PELLEGRINI-DE FRANCESCHIS-BENTIVOGLI-LAURENZA 2020.

53. UIF 2020.

12. settore commerciale/industriale di appartenenza riconducibile a quelli maggiormente a rischio di frode;
13. recente costituzione della società o recente “ingresso” nel settore commerciale/produttivo di riferimento: le società cartiere sono tipicamente di nuova costituzione o “quiescenti” e tornate nuovamente attive.

– Profilo oggettivo:

1. disposizioni di pagamento da/verso rapporti finanziari accesi all'estero o riconducibili a soggetti diversi dal cliente/fornitore sospettato di essere un *missing trader*;
2. «cessioni di beni a prezzi sensibilmente inferiori a quelli di mercato»⁵⁴;
3. inesistenza di uno “storico” nel settore di riferimento: la società cartiera è solitamente un *outsider* nel settore commerciale/produttivo in cui opera;
4. «offerta di affari con margini di profitto consistenti o predeterminati, indipendentemente da circostanze di tempo, quantità o qualità/natura delle merci o dei servizi commercializzati»⁵⁵;
5. assenza di contratti sottostanti alla fornitura di beni/servizi;
6. assenza di documentazione “accompagnatoria” delle forniture: ordini di acquisto, note di spedizione, lettere di vettura, CMR⁵⁶, sono documenti che consentono di risalire al reale fornitore/mittente dei beni, pertanto solitamente non vengono rilasciati da *missing trader*;
7. rapporti di *monocommittenza* tra sospetto “operatore mancante” e suo cessionario: la cessione di beni e la prestazione di servizi nei confronti di una sola impresa o di un numero estremamente limitato di imprese può essere indicativo della strumentalità dell'operatore in uno schema fraudolento;
8. presenza di pregiudizievoli “precedenti” fiscali e tributari;
9. acquisti di beni/servizi, senza applicazione dell'IVA, sulla base di false dichiarazioni d'intento.

In Tabella 1 [p. 27] sono schematicamente riepilogate le associazioni tra i concetti estrapolati

dagli elementi di anomalia sopra elencati e le rispettive classi che li rappresentano nell'ontologia MTO, con indicazione del profilo di appartenenza (soggettivo oppure oggettivo) e del numero progressivo con cui sono contraddistinti nei sopra riportati elenchi. Si noti che ad alcuni numeri progressivi del profilo soggettivo (n. 13) e del profilo oggettivo (nn. 1, 3, 5) corrispondono diversi concetti estratti dagli elementi di anomalia. Nel caso del n. 3 del profilo oggettivo, il concetto di “periodo di attività nel settore” che unitamente alle esperienze e capacità maturate concorre a formare lo “storico” di una società nel settore commerciale di competenza, è stato modellato dalla classe *OperatingSince*, già definita nel profilo soggettivo e contraddistinta dal n. 13.

Le classi contenute in Tabella 1 sono state quindi oggetto di generalizzazione e specializzazione. Le operazioni di generalizzazione sono state effettuate per “incapsulare” i concetti in *super-classi* connotate da superiore livello di astrattezza e maggiore genericità. Come già anticipato, l'approccio *bottom-up* seguito in questo caso è stato adottato con riferimento all'ontologia *top-level* DUL.

La Tabella 2 [p. 27], invece, riporta le generalizzazioni eseguite e le relative classi importate nell'ontologia MTO (campi “Classe MTO” e “Super-classe DUL (1)”). Poiché ogni *super-classe* di DUL è a sua volta “figlia” di un'ulteriore classe sovraordinata, sono state importate le rispettive classi “genitori” (campi “Super-classe DUL (2)” e “Super-classe DUL (3)”). Nessun concetto ha necessitato di estendere la propria generalizzazione ad una profondità maggiore di 3.

Le classi *Price*, *Capability* e *Reliability* non sono state riportate in Tabella 2 poiché non hanno *super-classe* in DUL; sono state “incapsulate”, infatti, in una classe creata *ad hoc* per contenere concetti che esprimono valori o qualità intrinseche del concetto stesso.

La classe così definita è stata denominata *ValuePartition* e include la *reificazione* di qualità e proprietà astratte, a loro volta serventi da “contenitori” per dati reali.

54. UIF 2020.

55. HM REVENUE & CUSTOMS 2020.

56. Acronimo di *Convention des Marchandises par Route*, è un documento emesso dal fornitore della merce o dallo spedizioniere che ne cura il trasporto, consistente in una lettera di vettura internazionale standardizzata.

Infine la Tabella 3 [p. 28] riporta la *gerarchia* delle sottoclassi di *ValuePartition*, mentre la Tabella 4 [p. 29] (specularmente a quanto riportato in Tabella 2) restituisce il prodotto dell'applicazione dell'approccio top-down alle classi di MTO sin qui presentate.

Oltre ad effettuare le opportune specializzazioni, per ragioni di completezza espressiva e di integrità della rappresentazione di alcuni elementi di criticità, sono state introdotte anche ulteriori classi utili a descrivere le caratteristiche tipiche dei *missing trader*.

Con riferimento ad una determinata classe di MTO, la stessa è stata distintamente inserita nella colonna "classe di specializzazione di MTO" o "classe introdotta per completezza" della Tabella 4, in base al fatto che la super-classe dalla quale "discende" fosse già presente o meno nell'ontologia (in fase di realizzo) dopo l'applicazione del metodo *bottom-up* e dopo la creazione della classe *ValuePartition*.

Tutte le classi componenti l'ontologia MTO, ad eccezione della classe "contenitore" *ValuePartition*, sono sottoclassi della classe *Entity* dell'ontologia DUL e, unitamente a questa, sono sottoclassi della classe *owl:Thing* (classe OWL predefinita, simbolicamente indicata dal simbolo *T*), la classe *radice* dell'ontologia e gerarchicamente superiore a tutte le altre classi (*C*) definibili ($\forall C, C \supseteq T$).

4.5. Descrizione semantica delle classi

Le ragioni che giustificano la creazione delle singole classi sinora introdotte sono racchiuse nella loro descrizione *semantica*.

Sono state dotate di annotazioni semantiche le sole classi non importate da DUL ed ogni descrizione è da intendersi strettamente contestualizzata nel dominio d'interesse. Al di fuori di tale dominio, infatti, alcuni concetti, descrizioni e annotazioni potrebbero assumere accezioni e connotazioni differenti:

Transaction: rappresenta una generica operazione di tipo commerciale o di tipo finanziario, legata alla compravendita di beni o servizi e posta in essere da due operatori economici. Costituisce uno dei concetti principali intorno a cui ruota l'ontologia del *missing trader*;

Payment: rappresenta l'atto del pagamento connesso alla conclusione di una compravendita

di beni o servizi; prevede un soggetto emittente ed un soggetto beneficiario del pagamento;

Amount: rappresenta una somma di denaro relativa ad un pagamento o a una transazione commerciale, riportata su un documento contabile (ad esempio una fattura) o finanziario (ad esempio una distinta di bonifico o una contabile bancaria);

Issuer: l'emittente di un documento (ad esempio una fattura) o di un pagamento (ad esempio un bonifico bancario);

Recipient: il destinatario di un documento (ad esempio una fattura) o il beneficiario di un pagamento;

Address: il generico indirizzo atto a localizzare un edificio che può fungere da sede per un soggetto giuridico (ad esempio l'indirizzo presso cui è ubicata la sede legale di una società, il suo domicilio fiscale o il luogo di esercizio dell'attività);

CorporatePurpose: rappresenta l'oggetto sociale di una società e più in generale le attività economiche che si propone di svolgere un soggetto giuridico;

Denomination: la denominazione di un soggetto giuridico. Può essere la ragione sociale di una società o la denominazione di una ditta individuale. È il nome con il quale è pubblicamente conosciuto un soggetto giuridico;

EstablishedSince: la data di costituzione di una società o di assegnazione della partita IVA per una ditta individuale;

LegalForm: la forma giuridica di una società o di un soggetto giuridico;

OperatingSince: la data a partire dalla quale è stata esercitata una determinata attività economica. Può non coincidere con la data di costituzione/attribuzione della partita IVA in quanto l'attività economica esercitata e l'oggetto sociale possono subire variazioni nel tempo;

ProfitMargin: rappresenta il margine di guadagno dato dalla differenza tra quanto ricavato da una fornitura e il costo sostenuto per l'acquisto a monte degli stessi beni. Fornisce un'indicazione sulla convenienza economica di una transazione;

RangeOfClients: è l'ampiezza della clientela di un determinato soggetto economico, può essere vasta e diversificata o ridursi ad una monocommittenza;

ShareCapital: il capitale sociale di una società;

Status: lo stato di attività in cui si trova un soggetto economico; può essere attivo, dormiente o cessato definitivamente;

VAT_Id: indica la partita IVA o il numero di registrazione IVA o il numero identificativo IVA con il quale è univocamente identificato un determinato soggetto passivo ai fini IVA. Il VAT_Id è emesso ed attribuito al rispettivo titolare solo ed esclusivamente dalle autorità fiscali dello Stato di residenza; è necessario, inoltre, ad abilitare il soggetto passivo ad effettuare operazioni intracomunitarie, previo inserimento nel VIES;

BusinessProfile: l'insieme di informazioni relative ad un soggetto giuridico desumibili dalla documentazione ufficiale reperibile su portali specializzati o autorizzati, come una visura camerale; tali informazioni possono essere coerenti o difformi rispetto a quanto appreso sul soggetto da diverse fonti;

CMR: è il modulo costituente una nota di spedizione in formato standardizzato, come stabilito dalla *“Convention relative au Contrat de transport international de Merchandises par Route”* (CMR), recante indicazioni su fornitore, spedizioniere, destinatario, luogo di consegna, quantitativo delle merci, ecc.;

Invoice: è il documento fiscale obbligatoriamente emesso da un soggetto economico, a fronte della realizzazione di una compravendita di beni/servizi, nei confronti di un committente, il quale è tenuto a corrisponderne il prezzo (indicato, per l'appunto, in fattura);

InvoiceSummary: costituisce il registro delle fatture attive e passive emesse e ricevute da un determinato operatore economico; fornisce informazioni che possono essere coerenti o incoerenti con quanto indicato dal soggetto nelle dichiarazioni fiscali o con il contenuto di eventuali dichiarazioni d'intento;

LetterOfIntent: è la dichiarazione d'intento mediante la quale un esportatore abituale palesa la propria intenzione di acquistare beni/servizi senza applicazione dell'IVA;

Order: l'ordine di acquisto sulla base del quale un fornitore cede della merce nei confronti del cliente. Solitamente è connesso o sostituisce un contratto di fornitura in cui fornitore e consumatore concordano precise condizioni;

ShippingNote: una nota di spedizione è un documento che accompagna il trasporto della merce fino a destinazione, emesso da chi ne cura la spedizione e contenente informazioni circa la merce trasportata. Ha un contenuto simile a quello di un CMR ma non ha un formato standardizzato;

TaxHistory: è la “storia” fiscale di un contribuente, fornisce indicazioni sul comportamento adottato dallo stesso nei confronti del fisco e mette in luce eventuali inadempienze;

BillofLading: la polizza di carico attesta l'imbarco della merce in un porto di origine e segue il trasporto fino al porto di destinazione, sostituendo una nota di spedizione solitamente utilizzata per i trasporti su terraferma. È un documento simile alla “bolla” di trasporto e al CMR, contenente informazioni sulla merce oggetto della spedizione;

Director: è l'amministratore di una società, il quale ha il potere di compiere atti di gestione dell'attività d'impresa e la sua funzione ha rilevanza internamente alla società ma non necessariamente verso i terzi;

LegalRepresentative: è il legale rappresentante, soggetto che assume su di sé la rappresentanza legale della società nei rapporti verso i terzi esterni all'azienda. Può coincidere o meno con l'amministratore;

Owner: con tale entità si è scelto di rappresentare il socio, unico o comproprietario di quote sociali, indipendentemente dall'eventuale carica/funzione rivestita all'interno della società;

TaxablePerson: nella Direttiva IVA un soggetto passivo⁵⁷ è colui il quale “esercita, in modo indipendente e in qualsiasi luogo, un'attività economica, indipendentemente dallo scopo o dai risultati di detta attività”. Di conseguenza, un soggetto passivo può essere una società, una ditta individuale o un professionista responsabile dell'applicazione, della riscossione e del versamento dell'IVA alle autorità fiscali;

MissingTrader: un'istanza di questa classe rappresenta la potenziale società cartiera al ricorrere di determinati “requisiti” (elementi di anomalia); introdotta principalmente per scopi legati alla validazione dell'ontologia, consente di interconnettere mediante opportune relazioni tutte le classi dell'ontologia MTO;

57. Cfr. art. 9 della Direttiva n. 2006/112/CE.

ValuePartition: classe “contenitore” creata per introdurre concetti astratti costituenti proprietà o caratteristiche che possono assumere valori “discreti” prestabiliti, utili alla descrizione dell'ontologia. Ad esempio la classe **LegalFormValue**, sottoclasse di **ValuePartition**, rappresenta il valore assumibile dalla forma giuridica di una società o più in generale di un soggetto giuridico. Sottoclassi di **LegalFormValue** sono infatti **LimitedCompany**, **CooperativeCompany**, **Simplified**, **SoleTrader**, le quali esprimono la “proprietà” di un soggetto giuridico di essere rispettivamente una società a responsabilità limitata, una società cooperativa, una società semplificata (più genericamente) o una ditta individuale. Come già rappresentato, sono stati valorizzati solo i concetti utili alla modellazione del dominio d'interesse; al di fuori di tale dominio **LegalFormValue** potrebbe assumere valori diversi (cioè avere altre sottoclassi, ad esempio “società per azioni” o “società di persone”). Costituendo (liste di) valori prestabiliti, sufficienti per la descrizione di un concetto, saranno legati a quest'ultimo da apposite relazioni che verranno definite nel prosieguo.

Per la descrizione semantica delle 61 sottoclassi della classe **ValuePartition**, trattandosi di concetti di uso comune il cui significato è facilmente intuibile, si rimanda alla Tabella 3 in cui sono già state presentate.

4.6. Le relazioni nell'ontologia del *missing trader*

In OWL e, di conseguenza, in *Protégé* è possibile distinguere due tipi di relazioni: *object properties* e *datatype properties*. Le prime mettono in relazione due classi o, più precisamente, due individui (istanze) appartenenti alle rispettive classi; le seconde, invece, “collegano” un'istanza ad un dato primitivo (*data literal*), il quale può essere costituito ad esempio da una stringa, da un numero intero o da un valore booleano (“vero” o “falso”).

Le relazioni per l'ontologia in esame saranno costituite esclusivamente da *object properties* relative ai concetti formalizzati, mentre non saranno definite *datatype properties*.

I valori “discreti” contenuti nelle sottoclassi di **ValuePartition**, infatti, sono tutti e soli i valori sufficienti ad “istanziare” le classi dell'ontologia.

La base di partenza delle *object properties* in MTO è stata ottenuta mediante importazione in

Protégé delle omologhe proprietà appartenenti all'ontologia *DUL*.

La “libreria” di relazioni importate, oltre ad essere agevolmente riutilizzabile, comprende alcune proprietà e le corrispondenti proprietà inverse (ad esempio *farFrom* e *nearTo*) particolarmente utili per esprimere diverse relazioni.

Per conferire maggiore chiarezza e una più lineare lettura di alcune proprietà, sono state comunque definite numerose relazioni integrative rispetto a quelle fornite da *DUL*; contrariamente, le proprietà dell'ontologia *top-level* non ritenute necessarie sono state ignorate.

Esempi di applicazioni in MTO di relazioni ereditate da *DUL* sono costituiti da *describes* e dalla sua *property* “inversa” *isDescribedBy* che mettono in relazione **BusinessProfile** (il profilo societario emergente dalle informazioni riportate in una visura camerale) con **TaxablePerson**; in tale contesto si sarebbe potuta utilizzare la macro-relazione *associatedWith* – anch'essa definita in *DUL* – ma si è ritenuto più opportuno esprimere una relazione di “descrizione” piuttosto di una relazione associativa, giacché comunemente una visura camerale offre una visione d'insieme sulla società ma non è un elemento ad essa strettamente associato, come potrebbero essere la denominazione o la partita IVA.

Ancora una volta, per modellare le relazioni necessarie, è apparso ragionevole partire dagli elementi di criticità/anomalia peculiari delle società cartiere.

Ad esempio, considerando l’“inesistenza della partita IVA” – elemento di criticità contraddistinto dal numero 1 nel profilo soggettivo del *missing trader* – il requisito espresso suggerisce l'istituzione di una relazione tra la classe che modella la partita IVA (**VAT_Id**) e la classe **Lack** (traducibile in “assenza” o “mancanza”), sottoclasse di **Existence** (a sua volta sottoclasse di **ValuePartition**) per rappresentare la relazione di effettiva “inesistenza” o “mancanza” di un'istanza di **VAT_Id**. Tale relazione è stata rappresentata dalla *object property* *hasExistence*, aggiunta alle relazioni già previste dall'ontologia *DUL*.

Analogamente, per ogni classe di **ValuePartition** è stata introdotta una corrispondente *object property* che mette in relazione una sottoclasse di **Entity** e una sottoclasse di **ValuePartition** avente attinenza

logica con la relazione stessa. Ad esempio la classe `LegalForm` è stata messa in relazione con la classe `LegalFormValue` per mezzo della object property `hasLegalFormValue`; in questo modo il concetto astratto di “forma giuridica” è stato connesso ad un valore ben definito (ad esempio “società a responsabilità limitata”) tramite un’opportuna relazione.

Nella definizione delle relazioni, osservando da una prospettiva matematico-insiemistica, si può assumere che esse mettono in correlazione individui (classi) appartenenti ad un dominio (*domain*) con individui appartenenti ad un codominio (*range*).

L’asserzione avente ad oggetto la dichiarazione di *domain* e *range* per una data proprietà ha permesso di dedurre nuova conoscenza: ad esempio, per la relazione `identifies`, una volta definito il dominio, costituito dalla classe `VAT_Id`, ed il codominio, costituito dalla classe `TaxablePerson`, la sua “inversa” `isIdentifiedBy` ha automaticamente acquisito come dominio `TaxablePerson` e come codominio `VAT_Id`, pur non avendolo asserito esplicitamente.

Tra le classi aventi caratterizzazione opposta è stata dichiarata la disgiunzione delle stesse (`Disjoint With`).

Ove necessario, le relazioni sono state definite come “functional”, connotazione che appone alla relazione in esame il vincolo che ad ogni esemplare del dominio (nel caso di specie `VAT_Id`) corrisponda uno ed un solo esemplare del codominio (o `Lack` o `Presence`).

Infine, per far sì che le relazioni in tal modo definite non “puntassero” alla super-classe astratta (ad esempio `Existance`) ma alle classi espressioni “valori concreti” (ad esempio `Lack` o `Presence`), è stato asserito che la super-classe di riferimento è equivalente alternativamente (“`Equivalent To`”) all’una o all’altra sottoclasse (“`Lack or Presence`”).

Un costrutto di questo tipo è detto *covering axiom* e serve a specificare che la super-classe non è semplicemente un “contenitore” per le sue sottoclassi ma è composta solo ed esclusivamente dagli individui appartenenti a quelle sottoclassi; in altre parole nella super-classe non c’è spazio per individui che non rientrino in una delle sottoclassi oggetto dell’assioma di equivalenza.

In Tabella 5 [p. 31] sono riportate le relazioni create *ad hoc* e quelle ereditate dall’ontologia DUL.

Sebbene non tutte le *object properties* di cui alla Tabella 5 siano strettamente utili allo scopo di rivelare l’operato di un *missing trader*, sono state comunque create per ragioni di completezza informativa e per conferire ad ogni concetto dell’ontologia una propria dimensione semantica. Ad esempio la relazione `hasName` non ha alcun ruolo nel processo inferenziale di rilevamento di una società cartiera ma è stata comunque definita, essendo la denominazione un elemento imprescindibile per l’identificazione di un soggetto.

4.7. Restrizioni sulle proprietà di MTO

La definizione di relazioni tra le classi equivale ad esprimere proprietà sulle classi stesse e consente di introdurre vincoli o restrizioni sugli individui di una classe (*property restrictions*), le quali hanno la funzione di descrivere formalmente la classe cui si riferiscono, esprimendo le condizioni necessarie affinché un individuo appartenga a quella classe.

In aggiunta alle asserzioni del tipo “`SubClass Of`”, “`Equivalent To`” e “`Disjoint With`” che predicano su una determinata classe indicandone, rispettivamente, la super-classe, le classi equivalenti e le classi disgiunte, è infatti possibile (e necessario) fare ricorso ad alcune altre restrizioni.

A partire dalle relazioni definite e riepilogate nella Tabella 5 è stato possibile applicare le opportune restrizioni alle classi dell’ontologia MTO, di cui si fornisce un esempio in Figura 1.

4.8. Creazione dell’entità *MissingTrader*

I concetti corrispondenti agli elementi di anomalia che accompagnano la società cartiera durante la sua “esistenza”, come si è visto, sono stati tradotti in linguaggio ontologico.

Per la realizzazione del modello di *missing trader* si è proceduto, dunque, ad operare la congiunzione tra la sua entità astratta (la classe `MissingTrader`) e le restrizioni su di essa definite (*property restrictions*).

A differenza di quanto fatto per la classe “genitore” `TaxablePerson`, su cui sono state introdotte restrizioni in senso lato, per meglio descrivere la classe `MissingTrader` si è reso necessario prendere in considerazione i singoli valori attribuibili alle sue proprietà peculiari.

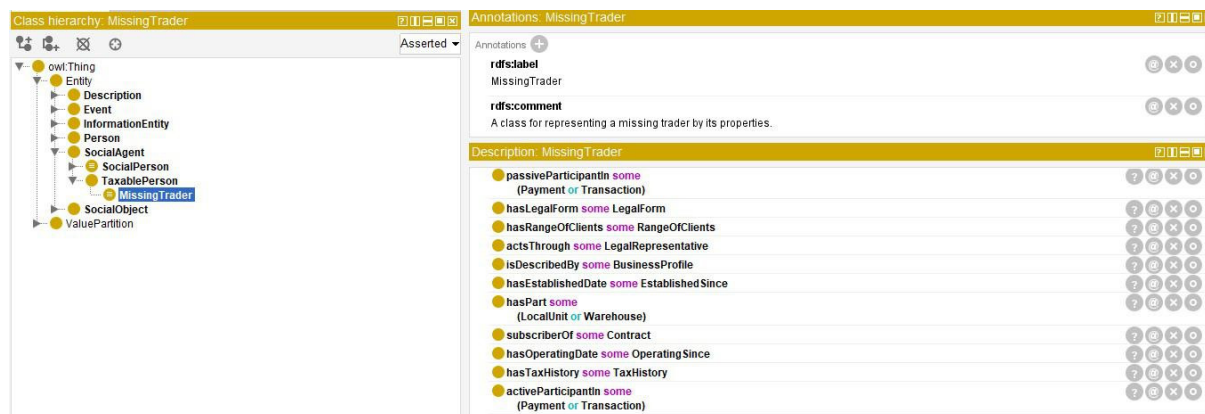


FIG. 1 — Restriction properties sulla classe MissingTrader in ambiente Protégé

Sebbene per alcune proprietà non fosse fondamentale esprimere una restrizione – ad esempio, per quanto attiene alla forma giuridica tipicamente assumibile dalle società cartiere, la classe *LegalFormValue* contiene tutti e soli i valori peculiari della società dal profilo “criminale” (*LimitedCompany*, *Simplified*, ecc.) – per altre è stato fondamentale operare una selezione che permettesse di distinguere il *missing trader* dal generico soggetto passivo IVA.

A tal fine si è fatto ricorso alle sottoclassi di *ValuePartition*, ove sono stati “isolati” tutti i valori (le classi) aventi accezioni coerenti con il profilo delle società cartiere e sono stati attribuiti all’entità in esame mediante le relazioni che li prevedevano come parte del proprio “insieme di arrivo” (*range*).

A mero titolo esemplificativo, con riferimento all’oggetto sociale del *missing trader*, tipicamente ampio, variegato e riferentesi ad almeno un settore commerciale considerato particolarmente a rischio di frodi, alla classe *MissingTrader* è stato attribuito un valore avente tale accezione e rappresentato dalla classe *Broad&Various&Risky* (appartenente alla sottoclasse *CorporatePurposeValue* di *ValuePartition*) mediante le relazioni *hasCorporatePurpose* e *hasCorporatePurposeValue*.

Il risultato della definizione delle restrizioni sulla classe *MissingTrader* è rappresentato da un set di assiomi, espressi in *sintassi di Manchester*.

Tali assiomi non rappresentano altro che l’introduzione nella classe *MissingTrader* delle definizioni degli elementi di criticità e di anomalia che la caratterizzano.

In tal modo è stata assegnata all’entità della società cartiera la connotazione necessaria per distinguerla da qualsiasi altro soggetto giuridico e al contempo per individuarla, tramite opportune “combinazioni” o “composizioni” di restrizioni.

4.9. Requisiti per l’individuazione di un *missing trader*

I profili soggettivo ed oggettivo delle società cartiere non rappresentano elenchi tassativi di caratteristiche che un soggetto passivo IVA deve possedere per poter essere qualificato come “operatore mancante”, piuttosto forniscono degli “indizi”, dettati dall’esperienza e dalle conoscenze maturate nel settore, al ricorrere dei quali si potrebbe essere in presenza di un *missing trader*.

Per contro, non si può pensare di individuare un *missing trader* sulla base di una sola delle anomalie che comunemente lo contraddistinguono.

Volendo esprimere tale osservazione in termini matematici, dunque, ai fini dell’individuazione di una società cartiera non è necessario che tutte le condizioni espresse dalle restrizioni si verifichino contemporaneamente e non è sufficiente che se ne verifichi una sola; bensì, è necessario e sufficiente che se ne realizzino alcune, purché significative.

Considerata la particolarità del dominio d’interesse, oggetto di costante evoluzione sotto il profilo normativo e fenomenologico, senza pretese di esaustività e di perentorietà, per il rilevamento di società cartiere è stato elaborato un modello basato su alcuni “capisaldi” selezionati tra gli elementi utili all’identificazione del *missing trader* (le cosiddette condizioni necessarie e sufficienti) e

sull'eventuale compresenza di situazioni altrettanto rilevanti ma meno determinanti.

Si è supposto che, per essere qualificato come tale, un "operatore mancante" dovesse rispondere almeno a due requisiti di carattere soggettivo – uno legato a dati "identitari" del soggetto e l'altro inerente ai suoi dati "societari" – e ad un requisito di carattere oggettivo, connesso alla sua operatività.

In relazione al profilo soggettivo, una caratteristica che ha un'altissima incidenza nel processo di rilevamento è rappresentata dalla forma giuridica del potenziale *missing trader* (dato "identitario"), unitamente alle pendenze tributarie/fiscali o al capitale sociale particolarmente esiguo o non interamente versato (dato "societario").

In relazione al profilo oggettivo, invece, un elemento più rappresentativo rispetto ad altri può essere dato dalla ridotta estensione della clientela del *missing trader*, spesso costituita da un solo

soggetto, oppure dall'inconsistenza di una eventuale dichiarazione d'intento in relazione al volume di operazioni commerciali compiute in un periodo temporale di riferimento.

L'opportuna combinazione di tali restrizioni, nell'esempio in esame, può (e dovrebbe) dunque restituire un requisito necessario e sufficiente per l'individuazione di una potenziale società cartiera.

Esprimendo in linguaggio logico le valutazioni appena esplicitate è possibile ricavare una sorta di "formula" o "regola" in cui i requisiti ritenuti maggiormente rilevanti per la qualificazione del *missing trader* possono essere interrelati tra loro e con i restanti elementi di criticità facendo ricorso agli operatori logici "AND" e "OR". Tale formula, espressa in uno pseudo-linguaggio logico-naturale, potrebbe essere rappresentata dalla seguente equazione:

("forma giuridica semplificata" AND ("oggetto sociale ampio, vario e a rischio" OR "data di costituzione recente" OR "sedi societarie soggette a frequenti variazioni" OR "altri elementi di anomalia di carattere soggettivo")) OR ((("capitale sociale esiguo o non versato" OR "inadempienze fiscali") AND (OR di "altri elementi di anomalia di carattere soggettivo"))) AND ((("clientela poco numerosa/diversificata" OR "dichiarazione d'intento inconsistente con altri dati contabili") AND (OR di "elementi di anomalia di carattere oggettivo"))) = "società cartiera";

dove i primi due blocchi di restrizioni – racchiusi tra doppie parentesi tonde e separati da "OR" – rappresentano i due requisiti di carattere soggettivo, con evidenza sul valore della forma giuridica, sul capitale sociale e sulla presenza di eventuali pendenze fiscali/tributarie, mentre l'ultimo blocco

– racchiuso tra doppie parentesi tonde e preceduto da "AND" – rappresenta il requisito di carattere oggettivo con evidenza sull'ampiezza del bacino di clienti e sulla inconsistenza di eventuali dichiarazioni d'intento (Figure 2 e 3).

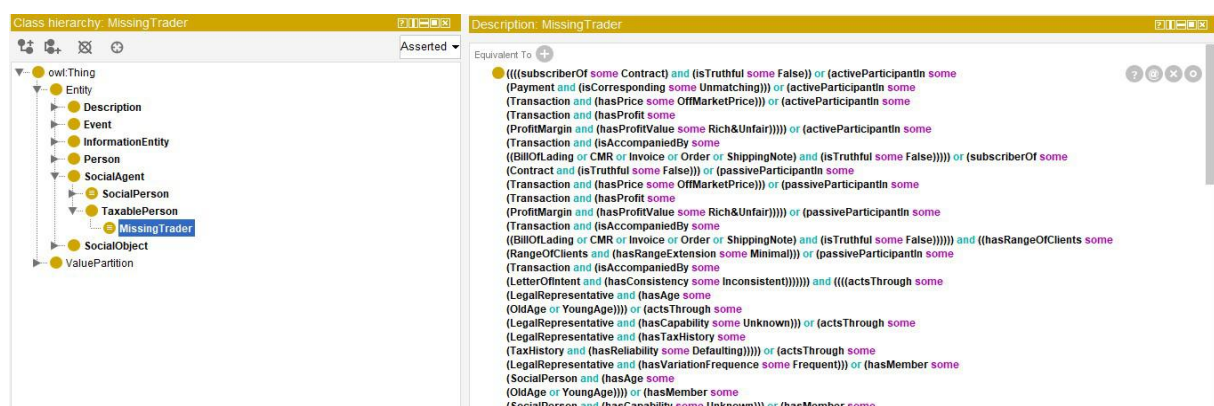


FIG. 2 — Combinazione di restrizioni definite sulla classe *MissingTrader* (parte 1 di 2)



5.1. Validazione dell'ontologia

Il processo di *validazione* consiste in un “controllo di conformità” basato sulla constatazione della *coerenza* e della *consistenza* dell'ontologia, caratteristiche che attengono alla concordanza e alla validità degli assiomi in essa definiti.

Protégé è dotato di *reasoner*, uno strumento di ragionamento automatico, ed è in grado di processare le ontologie per testarne coerenza e consistenza ma anche di inferire nuova conoscenza; in

Banali inferenze logiche sono state ottenute durante la fase di definizione delle relazioni in MTO, quando il *reasoner* di Protégé ha restituito dominio e codominio di una *object property* a partire dalla definizione di dominio e codominio della sua relazione inversa. Altri esempi di conoscenza (inizialmente ignota) dedotta da fatti noti sono costituiti dalla rivelazione di rapporti gerarchici tra le classi.

L'avvio del *reasoner* Pellet su MTO, alla ricerca di incoerenze e/o inconsistenze all'interno dell'ontologia e dei suoi assiomi, ha dato esito negativo (Figura 4).



Avendo constatato, dunque, che MTO è coerente e consistente è stato possibile testarne anche il corretto funzionamento.

5.2. Rilevamento del *missing trader* con uno strumento di ragionamento automatico

Il test dell'ontologia in esame ha preso le mosse dalla definizione della classe del *MissingTrader*.

L'aver costituito una *defined class* infatti, a patto di soddisfare le condizioni necessarie e sufficienti per l'appartenenza alla classe stessa, rende possibile la valutazione sull'idoneità di un dato individuo a popolare tale classe.

A tal fine, nell'interfaccia applicativa di Protégé, nella scheda "Individuals" dell'ontologia MTO, è stato creato un generico individuo (denominato "MExample"), senza dichiararne il "tipo" (ovvero l'appartenenza ad alcuna classe o super-classe) né fornendo alcuna altra descrizione sullo stesso, il quale dovrebbe costituire il potenziale *missing trader* (Figura 5).

Dopo aver creato il generico individuo, si è reso necessario assegnargli alcune proprietà. Tale processo ha richiesto la definizione di ulteriori individui, costituenti i concetti che le predette proprietà mettono in relazione. Le proprietà utili allo scopo sono costituite dalle condizioni necessarie e sufficienti definite nell'ambito della descrizione della classe *MissingTrader*.

Per la validazione dell'ontologia è stato fatto ricorso, quindi, all'espressione degli assiomi

descrittivi della classe *MissingTrader* per mezzo di relazioni ed individui delle opportune classi.

Il test condotto è stato basato sui seguenti elementi di anomalia:

- forma giuridica del soggetto connotata da "semplicità" – condizione rappresentabile creando un individuo delle sottoclassi di *LegalFormValue* e *LegalForm*;
- il soggetto è parte passiva (acquirente) in transazioni connotate da prezzi inferiori alla media di mercato – condizione rappresentabile facendo ricorso alle sottoclassi *OffMarketPrice* di *ValuePartition* e *Transaction* di *Entity*;
- il soggetto ha una clientela poco numerosa e diversificata o persino costituita da un solo cliente (monocommittenza) – condizione realizzabile tramite individui appartenenti alla sottoclasse *Minimal* di *RangeExtension* (in *ValuePartition*) e *RangeOfClients* (in *Entity*);
- il soggetto ha "pregiudizi" (Defaulting) di carattere fiscale/tributario (classe *TaxHistory*);
- oggetto sociale composto da attività rientranti in settori considerati a rischio frodi – situazione modellabile creando individui di *CorporatePurpose* e di *Broad&Various&Risky*;
- il legale rappresentante è un soggetto estraneo al settore di riferimento, la cui esperienza e capacità non sono note (individui *LegalRepresentative* e *Unknown*).

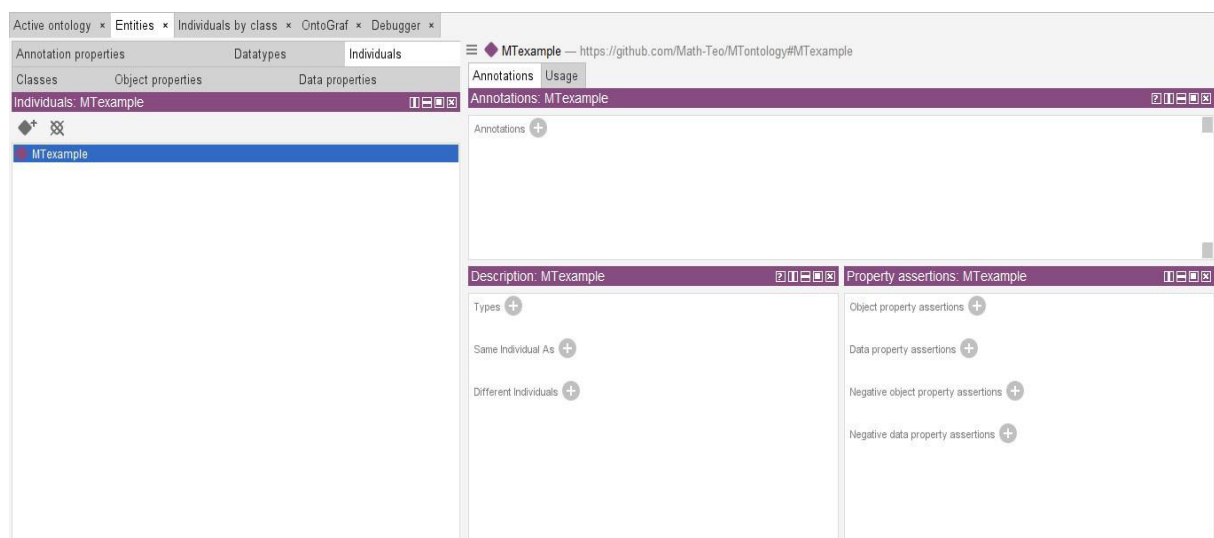


FIG. 5 — Creazione dell'individuo Mexample in ambiente Protégé

Nell'esempio, gli individui **LegalForm** (*formaGiuridica*) e **LegalFormValue** (*società Semplice* di tipo *Simplified*), sono messi in relazione da **hasLegalFormValue** (Figura 6); gli individui di tipo **Transaction** (*transazione*) e **OffMarketPrice** (*prezzo*) sono correlati mediante **hasPrice**; gli individui *monocommittenza* di tipo **Minimal** e *clientela* di tipo **RangeOfClients** sono connessi per mezzo della relazione **hasRangeExtension**; l'individuo *storico* di tipo **TaxHistory** è in relazione con *inadempiante* di tipo **Defaulting**; l'*oggettoSociale* rientra tra quelli a rischio (*aRischio*) tramite la relazione **hasCorporatePurposeValue** infine *legaleRappresentante* è *inesperto* (classe **Unknown**) grazie a **hasCapability**.

Dopo aver definito le relazioni tra gli individui si è proceduto col metterli in relazione con l'esemplare *MTexample*:

- **hasLegalForm** *formaGiuridica*;
- **passiveParticipantIn** *transazione*;
- **hasRangeOfClients** *clientela*;
- **hasTaxHistory** *storico*;
- **hasCorporatePurpose** *oggettoSociale*;
- **actsThrough** *legaleRappresentante*.

Infine è stato avviato il *reasoner Pellet* che ha correttamente e automaticamente dedotto la natura di *missing trader* del soggetto in esame (Figura 7).

5.3. Discussione dei risultati

Il risultato ottenuto (Figura 7) rispecchia pienamente le aspettative e convalida la correttezza degli assiomi espressi nell'ontologia: una volta definite



FIG. 6 — Creazione dell'individuo *formaGiuridica*, messo in relazione con l'individuo *societàSemplice* tramite la relazione **hasLegalFormValue**

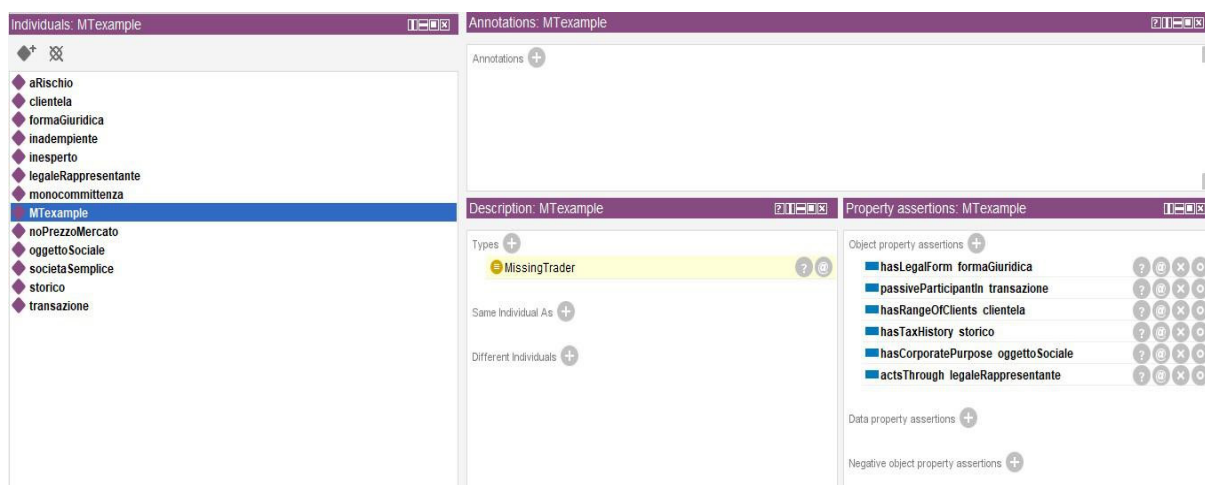


FIG. 7 — Individuazione del *missing trader* tramite inferenza logica con reasoner Pellet

le condizioni necessarie e sufficienti per la qualificazione di un *missing trader*, l'elaborazione del contesto operativo da parte di uno strumento di ragionamento automatico consente di rivelare la presenza di una potenziale società cartiera.

Si noti come gli elementi di anomalia su cui si è basato il test, nonché quelli definiti nell'ambito della classe *MissingTrader*, se valutati singolarmente non sono palesemente riconducibili alla fattispecie di società in esame: l'oggetto sociale a rischio frodi, la forma giuridica semplificata o ancora l'"estraneità" del rappresentante legale al settore commerciale di riferimento, sono fattispecie comuni a innumerevoli soggetti giuridici che operano regolarmente.

È tutt'altro che banale, quindi, che sia possibile discernere il profilo di operatività di un soggetto giuridico sulla base di tali (pochi) elementi informativi, seppur opportunamente interrelati.

Un'ulteriore contro-prova a sostegno della validità dell'ontologia e delle "regole" della classe *MissingTrader* è stata effettuata semplicemente facendo venire meno una delle condizioni necessarie affinché un soggetto passivo sia qualificabile come *missing trader*.

Ad esempio, scegliendo di eliminare la relazione "*MTexample hasRangeOfClients clientela*", il *reasoner Pellet* ha inferito nuova conoscenza, di carattere opposto rispetto a quella ottenuta nel primo test (Figura 8).

In questo caso è stato correttamente dedotto che non vi sono tutte le condizioni necessarie per l'individuazione di una società "cartiera", attribuendo all'individuo *MTexample* i connotati del generico *TaxablePerson* (soggetto passivo).

6. Conclusioni

Il presente contributo, pur nella sua essenzialità e senza pretese di esaustività e completezza, rappresenta un primo tentativo di applicazione di un sistema *ontology-based* per la prevenzione delle cosiddette MTIC VAT fraud.

Le condotte preventive rappresentano la fase propedeutica e, al tempo stesso, l'alternativa alla ricerca e alla repressione delle frodi. L'approccio ontologico, dal canto suo, offre potenzialmente infinite possibilità, essendo facilmente scalabile, integrabile ed estremamente versatile.

Se adottato in ambito unionale potrebbe dare impulso allo sviluppo di applicazioni perfezionabili dagli esperti del dominio d'interesse e sulla base delle più svariate esigenze.

Si tratta, dunque, di uno strumento universale e allo stesso tempo personalizzabile, utile a garantire uniformità nel trattamento del fenomeno senza trascurare il carattere prettamente territoriale di talune fattispecie criminose.

Se appare complicato uniformare il sistema investigativo e repressivo dei singoli Stati membri, si ritiene più facilmente realizzabile la convergenza da parte delle Autorità e delle Organizzazioni nazionali verso un modello inteso del problema, al fine di attuare quella cooperazione da sempre invocata e richiesta ma ad oggi mai pienamente concretizzata.

Incardinandosi in tale contesto, *Missing Trader Ontology* dimostra come, sulla base di informazioni facilmente e prontamente reperibili, sia possibile instaurare un principio di *predictive analytics*, fornendo indicazioni concrete sull'eventualità che delle società cosiddette "cartiere" agiscano in danno delle finanze pubbliche.

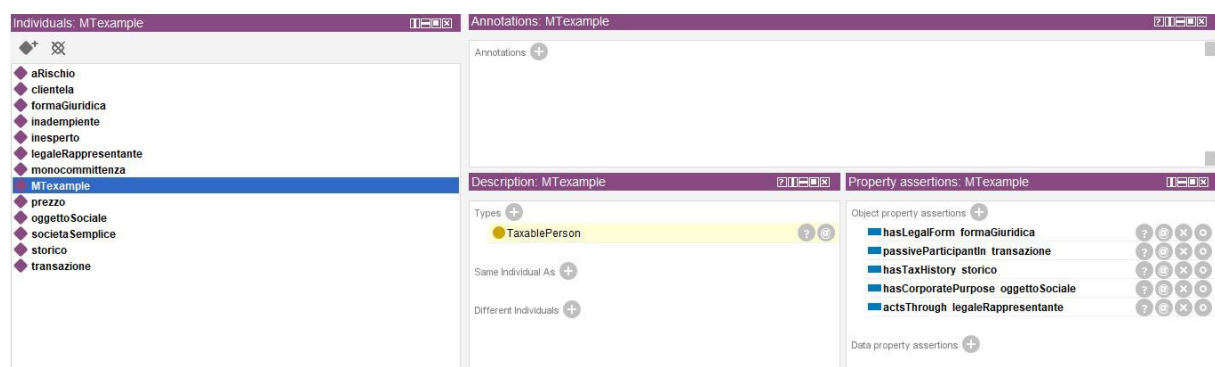


FIG. 8 — Nuova inferenza logica (contro-prova) sull'individuo *Mtexample* con reasoner *Pellet*

6.1. Propositi e sviluppi futuri

Per l'individuazione di fattispecie criminali caratterizzate da elevata complessità sarebbe opportuno far ricorso a regole altrettanto complesse, ad esempio redatte in linguaggio SWRL. Similmente a quanto avviene con gli assiomi e le asserzioni espresse in OWL, le regole SWRL possono essere trattate da un *reasoner*, come quello messo a disposizione da Protégé, per dedurre nuova conoscenza.

La futura integrazione di MTO potrebbe passare da un "ampliamento" della base di indicatori di criticità (quindi estendendo la classe *ValuePartition*), ricavando nuovi "requisiti" dal raffinamento di quelli esistenti, nonché introducendo diversi fattori di rischio volutamente lasciati nella realizzazione di questo progetto.

La valorizzazione dei concetti maggiormente rappresentativi dell'identità del *missing trader* potrebbe basarsi sull'uso di "pesi" per incrementarne o diminuirne la rilevanza, seguendo l'evoluzione del contesto giuridico-economico di riferimento o di eventuali necessità investigative.

La disponibilità di grandi quantità di dati potrebbe dare impulso a una sorta di *data driven innovation* anche nell'ambito investigativo, a patto che i dati siano analizzati efficacemente, come fatto in fase di costruzione dell'ontologia.

Si pensi a tutti gli indici di bilancio, ai dati derivanti dalle informazioni bancarie, alle informazioni apprese in seguito all'esperimento di determinati tipi di controlli fisici e materiali o separate indagini; elementi costituenti un patrimonio informativo significativo, big data spesso già nella disponibilità delle Autorità giuridiche o finanziarie, che non necessariamente richiedono il ricorso a tecniche di data mining.

Potrebbero presentare profili di utilità, inoltre, sia l'implementazione di API (Application Programming Interface) maggiormente *user-friendly* per l'interrogazione del sistema ontologico da parte di utenti non esperti del settore, sia la realizzazione di *endpoint* da interrogare e mettere a disposizione degli apparati statali per coadiuvare gli investigatori nello svolgimento delle indagini.

Tabelle

Profilo	N. progressivo	Concetto anomalia/criticità	Classe MTO
soggettivo	1	Partita IVA/numero identificativo IVA	VAT_Id
soggettivo	2	Forma giuridica	LegalForm
soggettivo	3-4-6	Sedi societarie/luogo di esercizio/unità locali	Address
soggettivo	5-12	Oggetto sociale/attività esercitate	CorporatePurpose
soggettivo	7	Capitale sociale	ShareCapital
soggettivo	8-9-10-11	Cariche sociali e di rappresentanza	SocialPerson
soggettivo	13	Data di costituzione	EstablishedSince
soggettivo	13	Periodo di attività nel settore	OperatingSince
oggettivo	1	Mittente pagamento	Issuer
oggettivo	1	Destinatario pagamento	Recipient
oggettivo	2	Prezzo di cessione	Price
oggettivo	3	Periodo di attività nel settore	OperatingSince
oggettivo	3	Capacità nel settore	Capability
oggettivo	4	Margine di profitto	ProfitMargin
oggettivo	5	Documentazione accompagnatoria	Contract
oggettivo	5-6	Documentazione accompagnatoria	InformationRealization
oggettivo	7	Estensione clientela (monocommittenza)	RangeOfClients
oggettivo	8	Affidabilità fiscale	Reliability
oggettivo	9	Lettera d'intento	LetterOfIntent

TAB. 1 — Associazioni classi-concetti nell'ontologia MTO

Classe MTO	Super-classe DUL (1)	Super-classe DUL (2)	Super-classe DUL (3)
VAT_Id	InformationObject	SocialObject / InformationEntity	Entity
LegalForm	InformationObject	SocialObject / InformationEntity	Entity
Address	InformationObject	SocialObject / InformationEntity	Entity
CorporatePurpose	InformationObject	SocialObject / InformationEntity	Entity
ShareCapital	InformationObject	SocialObject / InformationEntity	Entity
SocialPerson	Person	Entity	-
EstablishedSince	InformationObject	SocialObject / InformationEntity	Entity
OperatingSince	InformationObject	SocialObject / InformationEntity	Entity
Issuer	InformationObject	SocialObject / InformationEntity	Entity
Recipient	InformationObject	SocialObject / InformationEntity	Entity
ProfitManager	InformationObject	SocialObject / InformationEntity	Entity
Contract	Description	Entity	-
InformationRealization	InformationEntity	Entity	Entity
RangeOfClients	InformationObject	SocialObject / InformationEntity	Entity
LetterOfIntent	InformationRealization	InformationEntity	Entity

TAB. 2 — Generalizzazioni sulle classi dell'ontologia MTO

Sottoclasse di ValuePartition (X)	Sottoclasse della classe X
AddressType	AdministrativeOffice LegalOffice LocalUnit PlaceOfBusiness TaxDomicile Warehouse
Age	OldAge YoungAge
AuthorizationValue	VATregistered VIESregistered
Capability	Unknown Verified
Consistency	Consistent Inconsistent
CorporatePurposeValue	Broad&Various&Risky Simple&Restricted
Corresponding	Matching Unmatching
Existance	Lack Presence
LegalFormValue	CooperativeCompany LimitedCompany Simplified SoleTrader
Price	MarketPrice OffMarketPrice
ProfitValue	Fair Rich&Unfair
RangeExtension	Minimal Wide
Reliability	Compliant Defaulting
ShareCapitalValue	FullPaidUp MeagerOrUnpaid
StatusValue	Ceased Dormant Operating
TimeValue	Recent Dated
TruthValue	False True
Variation	Frequent Occasional

TAB. 3 — Classe ValuePartition e sue sottoclassi

Super-classe/i di DUL/MTO	Classe di specializzazione di MTO	Classe introdotta per completezza
Event - Action	-	Payment
Event - Action	-	Transaction
InformationObject	Amount	-
InformationObject	Denomination	-
InformationObject	Status	-
InformationRealization	BusinessProfile	-
InformationRealization	CMR	-
InformationRealization	Invoice	-
InformationRealization	InvoiceSummary	-
InformationRealization	Order	-
InformationRealization	ShippingNote	-
InformationRealization	TaxHistory	-
InformationRealization	BillOfLading	-
SocialPerson	Director	-
SocialPerson	LegalRepresentative	-
SocialPerson	Owner	-
SocialAgent	TaxablePerson	
TaxablePerson	MissingTrader	

TAB. 4 — Specializzazioni sulle classi dell'ontologia MTO

Object property	Ereditata (DUL)	Creata ad hoc	Domain	Range
activeParticipantIn		X	TaxablePerson	Payment or Transaction
actsFor	X		LegalRepresentative	TaxablePerson
actsThrough	X		TaxablePerson	LegalRepresentative
describes	X		BusinessProfile	TaxablePerson
farFrom	X		AddressType	AddressType
hasAddressType		X	Address	AddressType
hasAge		X	SocialPerson	Age
hasAmount		X	Invoice	Amount
hasAuthorizationValue		X	VAT_Id	AuthorizationValue
hasCapability		X	SocialPerson	Capability
hasChangeFrequency		X	Address	Variation
hasConsistency		X	LetterOfIntent	Consistency
hasConstituent	X		InvoiceSummary	Invoice
hasCorporatePurpose		X	TaxablePerson	CorporatePurpose
hasCorporatePurposeValue		X	CorporatePurpose	CorporatePurposeValue
hasEstablishedDate		X	TaxablePerson	EstablishedSince
hasEstablishedDateValue		X	EstablishedSince	TimeValue
hasExistance		X	VAT_Id	Existance
hasIssuer		X	Invoice	Issuer
hasLegalForm		X	TaxablePerson	LegalForm
hasLegalFormValue		X	LegalForm	LegalFormValue
hasLocation	X		TaxablePerson	Address
hasMember	X		TaxablePerson	SocialPerson
hasName		X	TaxablePerson	Denomination
hasNotAuthorizationValue		X	VAT_Id	AuthorizationValue
hasOperatingDate		X	TaxablePerson	OperatingSince
hasOperatingDateValue		X	OperatingSince	TimeValue
hasPart	X		TaxablePerson	LocalUnit / Warehouse
hasPrice		X	Transaction	Price
hasProfit		X	Transaction	ProfitManager
hasProfitValue		X	ProfitMargin	ProfitValue
hasRangeExtension		X	RangeOfClients	RangeExtension
hasRangeOfClients		X	TaxablePerson	RangeOfClients
hasRecipient		X	Invoice	Recipient
hasReliability		X	TaxHistory	Reliability
hasShareCapital		X	TaxablePerson	ShareCapital

Object property	Ereditata (DUL)	Creata ad hoc	Domain	Range
hasShareCapitalValue		X	ShareCapital	ShareCapitalValue
hasStatus		X	VAT_Id	Status
hasStatusValue		X	Status	StatusValue
hasTaxHistory		X	SocialPerson or TaxablePerson	TaxHistory
hasVariationFrequency		X	SocialPerson	Variation
identifies		X	VAT_Id	TaxablePerson
isAccompaniedBy		X	Transaction	BillOfLading or CMR or Invoice or LetterOfIntent or Order or ShippingNote
isConstituentOf	X		Invoice	InvoiceSummary
isCorresponding		X	Payment / VAT_Id	Corresponding
isDescribedBy	X		TaxablePerson	BusinessProfile
isHolderOf		X	Owner	ShareCapital
isIdentifiedBy		X	TaxablePerson	VAT_Id
isLinkedTo		X	Payment	Transaction / Price
isLocationOf	X		Address	TaxablePerson
isMemberOf	X		SocialPerson	TaxablePerson
isPartOf	X		Local Unit / Warehouse	TaxablePerson
issuerOf		X	Issuer	Payment or Transaction
isTruthful		X	Contract or BillOfLading or CMR or InvoiceSummary or Invoice or LetterOfIntent or Order or ShippingNote	TruthValue
managerOf		X	Director	TaxablePerson
passiveParticipantIn		X	TaxablePerson	Payment or Transaction
receiverOf		X	Recipient	Payment or Transaction
setUpFor		X	ShareCapita	TaxablePerson
subscriberOf		X	TaxablePerson	Contract

TAB.5 — Relazioni definite sull'ontologia MTO

Riferimenti bibliografici

- AGENZIA DELLE ENTRATE (2021), *Comunicato stampa*, 4 marzo 2021
- P. ALEXOPOULOS, K. KAFENTZIS, X. BENETOU et al. (2007), *Towards a generic fraud ontology in e-government*, in “Proceedings of the Second International Conference on e-Business – Volume 1”, 2007
- ALGEMENE REKENKAMER, BUNDESRECHNUNGSHOF, REKENHOF (2009), *Intra-Community VAT Fraud – Joint report*, 2009
- C. ANDREW, K. BAER (2023), *How to Combat Value-Added Tax Refund Fraud*, in “International Monetary Fund”, August 2023
- G. ATTIGERI, M.M.M. PAI, M. RADHIKA PAI, R. KULKHARNI (2018), *Knowledge Base Ontology Building For Fraud Detection Using Topic Modeling*, 2018
- F. BORSELLI (2008), *Pragmatic Policies to Tackle VAT Fraud in the European Union*, in “International VAT Monitor”, 2008, n. 5
- F.A. BUKHSH, H. WEIGAND (2015), *VAT Fraud: Possible technical and ontological solutions*, 2015
- CORTE DEI CONTI EUROPEA (2008), *Special Report n. 8/2007 concerning administrative cooperation in the field of value added tax*, 2008
- DIRETTORE DELL'AGENZIA DELLE ENTRATE (2023), *Provvedimento n. 156803/2023 del 16 maggio 2023*
- EUROPEAN COMMISSION (2023), *VAT gap in the EU: 2023 report*, 2023
- EUROPEAN COMMISSION (2020), *Study and Reports on the VAT Gap in the EU-28 Member States*, 2020
- EUROPEAN COMMISSION (2022), *VAT gap in the EU*, 2022
- EUROPEAN COMMISSION (2018), *The concept of tax gaps – Report III – MTIC fraud gap estimation methodologies*, 2018
- L. FANG, M. CAI; H. FU, J. DONG (2007), *Ontology-Based Fraud Detection*, 2007
- FATF/GAFI (2018), *Concealment of beneficial ownership*, 2018
- T.R. GRUBER (1993), *A translation approach to portable ontology specifications*, in “Knowledge Acquisition”, vol. 5, 1993, n. 2
- HM REVENUE & CUSTOMS (2020), *How to spot missing trader VAT fraud*, in “Gov.uk”, 31 December 2020
- A. HUSSAINI, Z. GUESSOUM, E. MERCIER-LAURENT (2022), *Elaboration of Financial Fraud Ontology*, in “Proceedings of the 17th Conference on Computer Science and Intelligence Systems”, 2022
- INTERNATIONAL VAT ASSOCIATION (2007), *Combating VAT Fraud in the EU. The way forward*, March 2007
- M. LAMENSCH, E. CECI (2018), *VAT fraud. Economic impact, challenges and policy issues*, Policy Department for Economic, Scientific and Quality of Life Policies – Directorate-General for Internal Policies, October 2018
- M.A. MUSEN (2015), *The Protégé project: A look back and a look forward*, in “AI Matters”, vol. 1, 2015, n. 4
- MINISTERO DELL'ECONOMIA E DELLE FINANZE (2022), *Documento di Economia e Finanza 2022. Rapporto sui risultati conseguiti in materia di misure di contrasto all'evasione fiscale e contributiva. Nota di Aggiornamento*. Allegato, 2022
- M. MOBILI (2022), *La UE rilancia la sfida contro l'evasione IVA: fattura elettronica in tutta Europa*, in “Il Sole 24 Ore”, 9 dicembre 2022

- R. NECHES, R.E. FIKES, T. FININ et al. (1991), *Enabling Technology for Knowledge Sharing*, in “AI Magazine”, vol. 12, 1991, n. 3
- A. OLTRAMARI, S. BORGO, C. CATENACCI, R. FERRARIO, A. GANGEMI, N. GUARINO, C. MASOLO, D. PISANELLI (2003), *Il ruolo dell'ontologia nella disambiguazione del significato*, in “Laboratory for Applied Ontology (LOA)”, 2003
- PARLAMENTO EUROPEO (2023), *Il mercato interno: principi generali*, 2023
- A. PELLEGRINI, P. DE FRANCESCHIS, C. BENTIVOGLI, E. LAURENZA (2020), *Un indicatore sintetico per individuare le società cosiddette cartiere*, in “UIF – Quaderni dell'antiriciclaggio”, 2020, n. 15
- TANG-LIU-YANG-WEI (2018), *Knowledge-based Financial Statement Fraud Detection System: based on an Ontology and a Decision Tree*, in “Knowledge organization”, vol. 45, 2018, n. 3
- G. TOSCHI (2018), *Linee d'azione e strategie del Corpo a contrasto delle frodi e dell'evasione fiscale*, in “Rivista della Guardia di Finanza 4”, 2018
- UIF – UNITÀ D'INFORMAZIONE FINANZIARIA PER L'ITALIA (2020), *Schemi rappresentativi di comportamenti anomali ai sensi dell'articolo 6, comma 7, lettera b), del D.Lgs. n. 231/2007*, novembre 2020
- W. VANDENBERGHE, B. SCHAFER, J. KINGSTON (2003), *Ontology Modelling in the Legal Domain – Realism Without Revisionism?*, 2003



RIVISTA ITALIANA DI
INFORMATICA E DIRITTO

PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0194 • articolo non sottoposto a peer review • pubblicato in anteprima il 13 dic. 2024
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale 

VINCENZO CALDERONIO

The state of the art of the Brazilian Bill on Artificial Intelligence with a focus on civil responsibility

Brazil is developing a regulatory framework for artificial intelligence (AI), which began in 2019 with a public consultation and culminated in Bill PL No. 2338/2023, under discussion in Parliament. This note outlines the state of the art, focusing particularly on the issue of civil responsibility.

Artificial Intelligence (AI) – Brazil – Regulation – Fundamental rights – Civil responsibility

Lo stato dell'arte del progetto di legge brasiliano sull'Intelligenza Artificiale con un focus sulla responsabilità civile

Il Brasile sta sviluppando un quadro normativo per l'intelligenza artificiale (IA), iniziato nel 2019 con una consultazione pubblica e culminato nel progetto di legge PL No. 2338/2023, in discussione in Parlamento. Questa nota presenta lo stato dell'arte, soffermandosi in particolare sul tema della responsabilità civile.

Intelligenza Artificiale (IA) – Brasile – Regolamentazione – Diritti fondamentali – Responsabilità civile

The Author is PhD candidate at the Department of Computer Science, University of Pisa and Institute of Legal Informatics and Judicial Systems of the National Research Council of Italy

Part of the research has been carried out at the *Centro de Tecnologia e Sociedade, Fundação Getulio Vargas* in Rio de Janeiro, Brasil

SUMMARY: 1. Introduction. – 2. Comparison with the AI Act. – 3. Civil responsibility framework. – 4. Conclusion.

1. Introduction

Brazil, like many other countries, is building its path toward artificial intelligence regulation.

It all started in December 2019 with a public consultation initiated by the Brazilian Minister of Science, Technology and Innovation to develop a strategy for artificial intelligence development. Shortly after, the Bill No. 21/2020 drafting rules for artificial intelligence was presented at the Chamber of Deputies¹.

Initially, the Bill only contained 10 articles, outlining the fundamental architecture of the proposal. The Chamber of Deputies accepted it in September 2021, advancing it to the Senate. On that occasion, much criticism arose due to the proposal's narrow scope compared to the EU Artificial Intelligence Act and its inability to create a wider horizon for the development of artificial intelligence systems in Brazil.

That criticism led to the new *projeto de lei* (PL) No. 2338/2023, which deploys a framework of 45 articles outlining normative provisions on the protection of fundamental rights (Chapter 2), risk categorization (Chapter 3), governance (Chapter 4) and civil responsibility (Chapter 5).

This is the proposal which was recently under examination in the Senate², where a Temporary Internal Commission of senators was formed in 2022 for the discussion with an original deadline of 8 August 2023 later extended to December 2024. On December 5th the Commission approved the

PL No. 2338/2023 that shifted to the Plenary where the Senate approved with modification the proposal on December 10th.

At this point the proposal will return to the Chamber of Deputies where another approval of the amended text will be needed for advancing it to the final stage.

In any case, Brazil will likely promulgate its first law on AI soon.

2. Comparison with the AI Act

Some general considerations can be made on the state of the art of PL No. 2338/2023 noticing how it has been influenced by the risk-based architecture of the EU AI Act and how, for certain aspects, it differs from it, reflecting also the difference of the two legal systems: Brazil, a federative system where the Parliament have full legislative competence and on the other side the European Union, an atypical legal system in development where the European Parliament have to divide its legislative power with the Parliaments of the Member States.

The Brazilian Bill adopts the EU approach by categorizing AI systems based on the risk that they pose for society, resulting in a tripartition of the AI system categorization into excessive, high and low levels of risk, mirroring the architecture of the AI Act³.

This choice came along with the definitions of AI system as a “computer system, with different degrees of autonomy” and provider as “a natural

1. Information regarding the *iter* of the legislative proposal, the Brazilian national strategy and an unofficial translation of the proposal can be found in BELLI-CURZI-GASPAR 2023.

2. See an [updated version of the proposal](#).

3. Some scholars may say that a *Brussels effect* occurred. For an analysis of the phenomenon see SIEGMANN-ANDERLJUNG 2022.

person or legal entity, of public or private nature, who develops an artificial intelligence system, directly or by order, aiming at placing it on the market” with clear reference to the AI Act semantical framework and the OECD principles of 2019.

However, apart from the fundamental architecture that somehow adopts the AI Act paradigm, major differences can be spotted.

A significant distinction is Brazil’s explicit inclusion of a section on fundamental rights, absent in the EU AI Act. While the AI Act protects fundamental rights in relation to economic interests, Brazil’s Bill places a direct emphasis on individual rights, introducing with article 6 of PL No. 2338/2023 provisions such as the right to explanation, the right to challenge AI system decisions and the right to human determination and human participation in decisions of artificial intelligence systems.

Indeed, fundamental rights are still protected in the AI Act, however, they’re protected in relation to economic interests, since the main assumption of the AI Act is that AI systems are regulated as products and most of the obligations that the AI Act pose are on the provider of the system.

This difference reflects also the aforementioned different institutional assets of the two countries, where in Europe the narrower scope of the legislation, focused only on the internal market regulation, is imposed by the partition of competence between the Union and the Member States ruled by the norms of the Treaty of Functioning of the EU.

Whereas most of those provisions are still present within the EU General Data Protection Regulation scope, in part expressly provided for such as Article 22 on automated decision-making and in part implicitly derived from the doctrine such as the right to an explanation⁴, it has been correctly argued that these norms apply solely in the case of personal data protection⁵. Brazil’s explicit remedies for individuals mark a broader recognition of AI’s societal impacts, which extend beyond the EU GDPR scope on personal data protection and the AI Act obligations for AI system design.

The Brazilian PL No. 2338/2023 expressly provides for remedies actionable by individuals such as Article 6(1), (2) and (3) on the right to con-

test decisions and to request human intervention, meaning that individuals will have new rights actionable for legal protection in courts.

Unfortunately, it should be noted that the AI Act does not expressly provide for remedies directly actionable by individuals, which are marginally treated by Chapter IX Section 4 on remedies, but instead creates a framework for market regulation obligations that mostly apply to businesses and providers of AI systems.

3. Civil responsibility framework

This normative difference is amplified by the provisions present in the Brazilian AI Bill on civil responsibility, which are instead absent in the EU framework, where a revision of the Product Liability Directive has been promulgated but without any introduction of norms on AI responsibility, which have instead been proposed in the context of the criticised AI Liability Directive⁶ whose future is currently uncertain.

Those choices confirm a European tendency to regulate these new technologies within the traditional framework of market regulation, missing the opportunity perhaps caught by Brazil to recognize a new normative paradigm in those technologies which establish a new type of relationship between people, rights and possible harms.

Still, a *Brussels effect* can be observed in the civil responsibility rules of the former Brazilian AI Bill, heavily influenced by the European Parliament Resolution of 20 October 2020. Even if those provisions changed in the latest version of the law that mixes part of the regime of the EU Parliament Resolution with an original system for the definition of the responsibility regime in concrete cases.

Indeed PL No. 2338/2023, after recalling the applicability of traditional norms for responsibility of the Código de Defesa do Consumidor and Código Civil, introduce in the *paragrafo único* of Article 36 a system for the definition in concrete of the regime of responsibility for AI.

This system is based on two criteria: the level of autonomy of the AI system correlated with its level of risk and the nature of the agent involved in the damage caused with AI.

4. SELBST-POWLES 2018.

5. ALMADA 2019.

6. HACKER 2024.

As a corollary, Article 37 empowers judges to reverse the burden of proof in cases of legal incapacity of the victim or when the excessive complexity of the AI system creates a *probatio diabolica*.

Delegating to the judiciary the authority to determine the applicable responsibility regime on a case-by-case basis appears to be an appropriate approach, adapting to a situation where, depending on the feature of the system and its relationship with individuals and their rights, different responsibility regimes could possibly apply to different applications of this technology.

A general clause delegating to judicial power the competence for responsibility avoids any potential error in the *ex-ante* allocation of a responsibility regime, leaving open the possibility of adopting the fault-based regime or the objective regime depending on the circumstances of the concrete case.

This choice reflects the fact that often it is not possible to state *ex-ante* if a certain system is a high or low risk, because the level of risk depends on the interaction of that system with society and this interaction should be verified in the actual case, meaning that a certain AI system could be qualified as high-risk in certain cases and low-risk in others depending on the interaction that it has with the environment and the fundamental rights implied in that particular interaction⁷.

The choice appears effective and resolves the problem of AI responsibility by asking the judicial system to qualify the AI system *ex-post* in trials and applying the consequent responsibility regime depending on that qualification.

4. Conclusion

In current times, where the civil responsibility regime for artificial intelligence in Europe is a debate fiercely disputed, a non-ideological approach such as the Brazilian one may be a good example that can lead to an effective solution of the problem by a case-by-case approach with an *ex-post* qualification of the fact made by the judicial system, avoiding the creation of additional certification bodies and ideological division between fault-based and objective responsibility.

However, this is only a sketch of the state of the art of the Brazilian Bill on artificial intelligence whose future will depend on the continuation of the legislative *iter* and future choices that will be made, shaping the future of AI regulation in Brazil and its global implications.

On this very last point, a recent modification of the proposal has been advanced in the Senate with Senator Eduardo Gomes as a relator, before the Plenary approval of December 10th, where some relevant modifications of the Bill have been introduced.

Notably, the Brazilian Senate purposefully adopted amendments with the scope of promoting the development of AI systems and applying a regulatory logic based more on *ex-post* considerations rather than *ex-ante*, differentiating itself from the European approach criticized by Draghi's Report on the Competitiveness of the Union, explicitly cited in the *complementação de voto* presented in the Senate.

This resulted in a modification of the regime for the preliminary risk assessment (Article 12), changing it from mandatory to optional. This modification was accompanied by the introduction of a general clause in Article 6 that adapts the protection of fundamental rights to the state of the art of technological development.

Lastly, some relevant modifications have been introduced concerning the Sistema Nacional de Regulação e Governança de Inteligência Artificial (SIA), which will be the competent authority for the enforcement, with powers to investigate high-risk AI systems in case of suspected violation of norms, including the power of accessing the documentation and the training data of the related AI system, whose authority became residual in this last modification.

These amendments raised concerns among scholars involved in the debate who talked of a weakening of the rights-based approach of PL No. 2338/2023, which shifted more to economic considerations of law.

Despite this criticism, the Brazilian AI Bill today may still be considered a new framework, grounded in the AI Act paradigm, which goes

7. For relevant considerations on civil responsibility for AI coming from Brazilian literature see SPADACCINI DE TEFFÉ-MEDON 2020 and MAGANHOTO DONEDA-SCHERTEL MENDES-PEREIRA DE SOUZA-GOMES DE ANDRADE 2018.

beyond its limits and that may represent a right-based regulation with individuals at its core, making Brazil a very interesting testing ground for the intersection between artificial intelligence and its social implications.

References

- M. ALMADA (2019), *Human intervention in automated decision-making: Toward the construction of contestable systems*, in “ICAIL ’19: Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law”, ACM, 2019
- L. BELLI, Y. CURZI, W.B. GASPAR (2023), *AI regulation in Brazil: Advancements, flows, and need to learn from the data protection experience*, in “Computer Law & Security Review”, vol. 48, 2023
- P. HACKER (2024), *Proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence: Complementary impact assessment*, EPRS - European Parliamentary Research Service, 2024
- D.C. MAGANHOTO DONEDA, L. SCHERTEL MENDES, C.A. PEREIRA DE SOUZA, N.N. GOMES DE ANDRADE (2018), *Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal*, in “Pensar. Revista de Ciências Jurídicas”, vol. 23, 2018, n. 4
- A. SELBST, J. POWLES (2018), *Meaningful Information and the Right to Explanation*, in “Proceedings of the 1st Conference on Fairness, Accountability and Transparency”, 2018
- C. SIEGMANN, M. ANDERLJUNG (2022), *The Brussels effect and artificial intelligence: How EU regulation will impact the global AI market*, arXiv preprint, 2022
- C. SPADACCINI DE TEFFÉ, F. MEDON (2020), *Responsabilidade civil e regulação de novas tecnologias: questões acerca da utilização de inteligência artificial na tomada de decisões empresariais*, in “Revista Estudos Institucionais”, vol. 6, 2020, n. 1



ELISA SORRENTINO – ANNA FEDERICA SPAGNUOLO

Cybersecurity e sovranità digitale nella protezione dei dati personali

Con la crescente complessità della tecnologia, la cybersecurity richiede un approccio integrato e multidisciplinare. Sebbene la tecnologia offra numerose opportunità, il suo rapido sviluppo ha introdotto tecniche sempre più invasive che hanno un impatto sia sulla sfera privata sia su quella pubblica. Inizialmente limitate ai sistemi informatici, queste problematiche riguardano ora i diritti fondamentali, la sicurezza delle infrastrutture e la sovranità degli Stati. In risposta ai rischi e alla complessità crescenti, sono necessarie misure legislative più ampie e mirate. In questo contesto, è fondamentale adottare una prospettiva di cybersecurity che trascenda il dominio puramente tecnico, coinvolgendo il discorso giuridico e politico sulla sovranità digitale e la protezione dei dati. L'obiettivo è promuovere una cybersecurity che garantisca la sicurezza dei dati e delle informazioni nel pieno rispetto dei diritti fondamentali sanciti da standard più elevati e universalmente validi.

Cybersecurity – Sovranità digitale – Dati personali – Diritti fondamentali

Cybersecurity and Digital Sovereignty in Personal Data Protection

With the increasing complexity of technology, cybersecurity requires an integrated and multidisciplinary approach. Although technology offers numerous opportunities, its rapid development has introduced increasingly invasive techniques that impact both the private and public spheres. Initially limited to information systems, these issues now affect fundamental rights, infrastructure security, and state sovereignty. In response to growing risks and complexity, broader and more focused legislative measures are needed. In this context, it is crucial to adopt a cybersecurity perspective that transcends the purely technical domain, engaging the legal and political discourse on digital sovereignty and data protection. The goal is to promote cybersecurity that ensures data and information security while fully respecting fundamental rights enshrined in higher and universally valid standards.

Cybersecurity – Digital Sovereignty – Personal Data – Fundamental Rights

Le Autrici afferiscono all'Istituto di Informatica e Telematica del CNR, sede di Cosenza

Questo lavoro è il risultato di una ricerca comune e condivisa condotta da entrambe le Autrici ed è stato parzialmente realizzato nell'ambito delle attività del progetto "Security and Rights in the CyberSpace – SERICS (PE00000014)" – Piano Nazionale di Ripresa e Resilienza MUR finanziato dall'Unione europea – NextGenerationEU, CUP B53C22003950001

Un particolare ringraziamento è rivolto al prof. Domenico Talia per aver fornito preziosi consigli e interessanti spunti di riflessione sull'impatto che i modelli predittivi e gli algoritmi di *machine learning* possono avere su decisioni e comportamenti umani

SOMMARIO: 1. Introduzione. – 2. Dall'indipendenza del cyberspazio alla sovranità digitale. – 3. La sfida della cybersecurity: protezione dei dati e normative nell'era delle violazioni informatiche. – 4. Sovranità digitale e cybersecurity: sinergia a tutela dei diritti nell'era delle crisi globali. – 5. Conclusioni.

1. Introduzione

Per instaurare un clima di fiducia nel complesso e dinamico cyberspace¹, la cybersecurity, considerata la crescente estensione del suo campo d'azione, richiede un approccio multidisciplinare e integrato². Sebbene la tecnologia offra significative opportunità di progresso, miglioramento culturale, sanitario, tecnologico ed economico, il suo sviluppo rapido e pervasivo facilita difatti l'emergere di tecniche e modalità sempre più invasive, incidendo sia sulla vita privata dei cittadini sia sulla sfera dell'attività pubblica.

Le criticità originariamente connesse esclusivamente ai sistemi informatici e alle reti di comunicazione³ oggi manifestano effetti pervasivi e

reticolari, impattando significativamente sui diritti fondamentali e sulle libertà delle persone⁴, sugli equilibri politici e sulla sicurezza di infrastrutture, ponendo sfide inedite alla sovranità degli Stati.

Per di più, l'aumento della tipologia dei rischi è accompagnato da una proporzionale crescita degli attori coinvolti e dalla complessità delle tecnologie sviluppate. Questo contesto determina un cambio di paradigma che richiede, da parte del legislatore nazionale e internazionale, risposte molteplici e diversificate.

A questo si aggiunge la proliferazione normativa degli ultimi anni, spesso ancora in fase di attuazione, che ha consolidato un'architettura di sistema estremamente vasta e variegata, generando

1. MARTINO 2018, p. 66. L'autore scrive che la *National Military Strategy for Cyberspace Operations* (NMS-CO) del 2006 ha descritto il cyberspazio attraverso l'acronimo VUCA, ossia: *Volatility, Uncertainty, Complexity, Ambiguity*.
2. In questo senso il Rapporto CLUSIT (Associazione Italiana per la sicurezza informatica) per l'anno 2016, p. 12 definisce la cybersecurity come «il gruppo di attività e competenze multidisciplinari, complesse e sofisticate, molte delle quali non informatiche, che sono oggettivamente di difficile integrazione con le prassi esistenti [...] costruite negli anni a partire da esigenze di compliance».
3. Commissione europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale e al Comitato delle regioni - *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo* (COM/2001/0298). Creare una società dell'informazione sicura per l'Ue significa migliorare la sicurezza delle infrastrutture dell'informazione ma anche lotta alla criminalità informatica. Si veda Commissione delle Comunità Europee, Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato Economico e Sociale e al Comitato delle Regioni - *Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica* (eEurope 2002), Bruxelles, 26 gennaio 2001 COM(2000) 890, e la Direttiva 90/387/CEE del Consiglio, del 28 giugno 1990, sull'istituzione del mercato interno per i servizi delle telecomunicazioni mediante la realizzazione della fornitura di una rete aperta di telecomunicazioni (*Open Network Provision* - ONP).
4. ESPOSITO 2019.

inevitabili difficoltà applicative e onerosi sforzi nel recepimento da parte degli Stati membri.

Uno degli ostacoli più significativi è rappresentato dall'uso di un linguaggio tecnico giuridico settoriale, che crea barriere comunicative e ostacola l'armonizzazione normativa.

La diversità delle esigenze dei vari ordinamenti nazionali rende particolarmente ardua la creazione di un quadro regolatorio euro unitario coeso ed efficace, specialmente in settori altamente specialistici.

Questa difficoltà è particolarmente accentuata nel campo della protezione dei dati personali⁵, in cui l'armonizzazione tra le disposizioni sovranazionali e nazionali richiede un'importante fase di interpretazione e coordinamento che non sempre risulta agevole e spesso genera conflitti normativi⁶.

Per superare queste sfide, è auspicabile ripartire dal rispetto per la gerarchia delle fonti,

valorizzando i trattati internazionali che incorporano principi condivisi e utilizzano un linguaggio universale⁷.

Partendo da questo presupposto, con l'intento di facilitare un dialogo più fluido e produttivo tra le politiche interne e quelle sovranazionali, il presente lavoro sottolinea l'importanza cruciale di una concezione di cybersecurity che trascenda il mero confronto tecnico proiettandosi nell'attuale e complesso dibattito giuridico e politico sulla sovranità digitale⁸ in relazione alla protezione dei dati personali. L'intento è di offrire una visione di cybersecurity inserita in un contesto di sovranità digitale, la cui legittimazione ultima risiede nella capacità di garantire la sicurezza dei dati⁹ e delle informazioni, in piena ottemperanza ai diritti fondamentali sanciti da norme di rango superiore e valide *erga omnes*¹⁰.

5. L'art. 4, paragrafo 1, del Regolamento Generale sulla Protezione dei Dati (GDPR) definisce con «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale». Si aggiunga che il Considerando 30 prevede che: «Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle».
6. Il GDPR impone standard rigorosi per la protezione dei dati personali. Tuttavia, l'applicazione uniforme di tali standard è resa difficile dalle differenti legislazioni nazionali e dalle interpretazioni divergenti delle stesse norme. Questa situazione richiede un'armonizzazione giuridica che spesso risulta conflittuale, con conseguenti difficoltà nell'attuazione di politiche coese.
7. Il Trattato di Lisbona e la Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione 108), rappresentano, a titolo esemplificativo, strumenti normativi fondamentali che offrono un quadro di principi e terminologie condivise a livello internazionale.
8. La sovranità digitale è stata finora definita in modo piuttosto vago. Recentemente è emersa la nozione «Europe's ability to act independently in the digital world». A tal proposito si veda MADIEGA 2020. Per una panoramica della letteratura in tema di sovranità digitale si rinvia all'analisi di HUMMEL-BRAUN-TRETTNER-DABROCK 2021. Gli autori identificano sei differenti nozioni di sovranità. Sull'argomento si veda, inoltre, MOEREL-TIMMERS 2021; SIMONCINI 2017, p. 19 ss.
9. Sull'argomento si veda, OROFINO 2022, pp. 82 ss., FINOCCHIARO 2014; PASSAGLIA 2016; PIZZETTI 2016, p. 9 ss.
10. Si veda CASSESE 2006. Nel testo si legge che: «Le norme [...] *erga omnes*, [...] presentano le seguenti caratteristiche: sono obblighi che proteggono valori fondamentali per la comunità internazionale nel suo insieme (pace, diritti umani, autodeterminazione dei popoli, protezione dell'ambiente); sono obblighi di natura solidale, nel senso che essi incombono su ogni membro della società internazionale nei confronti di tutti gli altri membri

Analizzeremo quindi l'evoluzione di una disciplina che, sebbene nata per garantire il corretto funzionamento e l'efficienza delle infrastrutture pubbliche e private, oggi è deputata a preservare l'esercizio dei diritti fondamentali¹¹ e a favorire uno sviluppo tecnologico sostenibile e rispettoso dei principi democratici¹² in risposta alle esigenze di una società moderna, democratica e partecipata¹³.

2. Dall'indipendenza del cyberspazio alla sovranità digitale

Nel 1996 la pubblicazione della Dichiarazione di indipendenza del *cyberspazio*¹⁴ fu dettata da un clima di generale entusiasmo per la rapidissima e travolgente rivoluzione digitale in corso. Fu in nome di una più ampia autonomia, di una diffusa libertà di opinione e di espressione, che i padri della rete e i loro giovani allievi «codificarono e scolpirono nella pietra l'antipatia per i governi e per la regolamentazione»¹⁵, disponendo di fatto l'assenza di autorità all'interno di questo ecosistema. Non era stato evidentemente previsto che i potenti del web avrebbero presto iniziato a dominare gli ampi spazi

geopolitici¹⁶ traendo grandi vantaggi dallo sviluppo di un *cyberspazio* privo di regole¹⁷, in cui i dati assumono sempre più velocemente il ruolo di fulcro in un nuovo archetipo di capitalismo estrattivo basato sulle piattaforme digitali¹⁸. Saranno il caso *Snowden*¹⁹ e lo scandalo *Facebook – Cambridge Analytica*²⁰ a evidenziare il pericolo indotto dall'utilizzo fraudolento dei dati personali degli utenti da parte di piattaforme multinazionali. Due episodi dal forte impatto mediatico che andranno ad agitare il dibattito politico sulla necessità di intervenire in maniera radicale a tutela dei diritti individuali nel contesto digitale garantendo maggiore privacy e sicurezza degli utenti. Il caso *Schrems* e il relativo dispositivo della Corte di Giustizia UE andranno invece a costituire il primo importante passo da un punto di vista giurisprudenziale per l'affermazione di una sovranità digitale dell'Unione europea²¹. La decisione della Corte andrà difatti a ribaltare l'orientamento decisivo nel caso *Google Spain* in cui era diversamente predominante la diffusa convinzione che il trattamento dei dati da parte del grande motore di ricerca, doveva ritenersi

(o, nel caso essi discendano da trattati, nei confronti di tutte le altre parti contraenti); ad essi corrisponde un diritto sostanziale che appartiene ad ogni membro della comunità internazionale (o ad ogni parte al trattato); l'azione a tutela di tale diritto è esercitata per conto dell'intera comunità internazionale o dell'insieme delle parti contraenti) per salvaguardare gli interessi fondamentali di quella comunità».

11. Si veda a tal proposito RODOTÀ 2006; POLLICINO-BERTOLINI-LUBELLO 2013.

12. BRIGHI-CHIARA 2021, pp. 11 ss.

13. Si veda a tal proposito SANTANIELLO 2022.

14. BARLOW 1996.

15. BERTOLA 2022.

16. Cfr. AMATO MANGIAMELI-CAMPAGNOLI 2020.

17. MANGIAMELI 2023-A, p. 281. Si veda inoltre SERINI 2023, e ancora WALKER 2015. Si veda ancora FRANZESE 2009.

18. Cfr. HARVEY 2006; FORMENTI 2008; ZUBOFF 2019.

19. Nel 2013, Edward Snowden, ex contractor dell'intelligence degli Stati Uniti, ha divulgato l'esistenza di riservatissimi programmi di sorveglianza globale condotti dall'agenzia governativa National Security Agency (NSA) accendendo un forte dibattito sulla privacy, sulla sorveglianza governativa e sul delicato equilibrio tra sicurezza nazionale e diritti individuali. Si veda a tal proposito DARNIS 2021. Lo scandalo Facebook – Cambridge Analytica ha messo in evidenza il pericolo dell'utilizzo fraudolento dei dati personali degli utenti da parte di piattaforme multinazionali. I dati di 87 milioni di utenti, di cui 2,7 milioni si trovano nell'Ue, potrebbero essere stati violati e usati impropriamente. Della vicenda si è occupato anche il Parlamento europeo.

20. Nel 2018 Christopher Wylie rivelò che Cambridge Analytica aveva ottenuto i dati personali degli utenti attraverso accordi con Aleksandr Kogan, creatore di un'app di Facebook che raccoglieva informazioni per scopi di ricerca. Cambridge Analytica ha poi utilizzato questi dati per influenzare e manipolare il voto in eventi chiave come la campagna per il referendum sulla Brexit e le elezioni presidenziali statunitensi del 2016, che hanno visto la vittoria di Donald Trump. Si veda a tal proposito FAINI 2019-A; SIMONCINI 2019.

21. ZENO-ZENCOVICH 2016.

effettuato sui *mainframe* presenti negli Stati Uniti, e quindi non fosse soggetto alla direttiva UE sui dati personali²². Inizia, in altri termini, a prendere forma la consapevolezza che sia necessario arginare una pericolosa idea di sovranità digitale mista “sia pubblica che privata” in cui la capacità di regolamentare i mercati e gestire la comunicazione pubblica sia delegata alle grandi multinazionali che forniscono le infrastrutture. Si impone come linea di indirizzo strategica la volontà di invertire quella medesima ambivalenza che rischia di proiettarsi anche sul mondo del diritto, spingendo verso il superamento della classica distinzione pubblico-privato²³. Dinanzi al timore di ulteriori minacce del tutto inedite²⁴ si afferma un evocativo concetto di sovranità digitale²⁵ da intendersi come la capacità di un Paese di esercitare autorità all'interno del *cyberspazio*, garantendo l'indipendenza tecnologica e il controllo sui dati personali. Sarà la Cancelliera tedesca Angela Merkel, nel luglio 2020, a lanciare per la prima volta l'idea di definire la sovranità digitale come tema centrale all'interno del suo programma ufficiale per la presidenza del Consiglio europeo prospettando l'implementazione di un'infrastruttura digitale europea ad

alte prestazioni, sovrana e resiliente²⁶. Questo è essenzialmente l'obiettivo del progetto europeo *Gaia X*²⁷, finalizzato a ridurre la dipendenza dalle piattaforme dei cloud extraeuropei²⁸ e a creare un ecosistema digitale aperto, trasparente e sicuro, in cui dati e servizi possano essere resi disponibili, raccolti e condivisi in un ambiente di fiducia. Lo scopo è quello di rintracciare forme di maggior tutela per l'autodeterminazione dei propri cittadini e delle imprese dinanzi alle sfide poste dall'ampio dispiegamento di tecnologie digitali altamente invasive, come l'intelligenza artificiale e l'“Internet delle cose”. Seguirà la progressiva affermazione della sovranità digitale come priorità strategica nell'agenda politica dell'Unione europea. Questo è testimoniato anche dai recenti pronunciamenti di Ursula von der Leyen²⁹. La Presidente della Commissione europea, in un'ottica di rinnovato impegno verso la costruzione di un'Europa più verde, digitale e resiliente sottolinea l'esigenza di plasmare un continente in cui i cittadini possano liberamente esprimere la propria identità, coltivare le proprie aspirazioni e relazioni interpersonali, in linea con i principi fondanti delle democrazie liberali³⁰.

22. *Ibidem*.

23. SIMONCINI-CREMONA 2022, p. 258.

24. Si veda a tal proposito SIMONCINI 2017.

25. Per una panoramica della letteratura in tema di Sovranità Digitale si rinvia all'analisi di HUMMEL-BRAUN-TRETER-DABROCK 2021. Gli autori identificano sei differenti nozioni di sovranità. Sull'argomento si veda, inoltre, MOEREL-TIMMERS 2021; SIMONCINI 2017. Si veda inoltre FINOCCHIARO 2022.

26. Dal sito della Presidenza tedesca del Consiglio dell'Unione europea si veda: *Secure and sovereign, European-based, resilient and sustainable digital infrastructure is essential to this transformation*.

27. Il progetto europeo *Gaia X* ha come obiettivo principale la creazione di un'infrastruttura cloud che rafforzi la sovranità digitale, la competitività e il peso politico dell'EU attraverso la creazione di “data space”, “spazi di dati” in grado di trasporre in forma digitale gli ecosistemi fisici, naturali, industriali o sociali già esistenti all'interno dell'Unione europea.

28. Si veda a tal proposito AUTOLITANO-PAWLOWSKA 2021 o ancora il Dossier *The Gaia-X Ecosystem - A Sovereign Data Infrastructure for Europe*.

29. La Presidente von der Leyen nella sessione plenaria del Parlamento europeo ha evidenziato come «Nulla di tutto ciò è fine a sé stesso: è in gioco la sovranità digitale dell'Europa, sia su piccola che su larga scala». Per approfondimenti si veda il discorso sullo stato dell'Unione.

30. In questo solco, la Presidente von der Leyen ha delineato una serie di iniziative volte a rafforzare gli elementi costitutivi del Green Deal europeo proiettando l'Unione verso una trasformazione digitale che sia rispettosa dei diritti fondamentali degli individui. Tale approccio si inserisce in una più ampia strategia di democratizzazione e costituzionalizzazione della rete, finalizzata a limitare l'esercizio del potere da parte delle grandi piattaforme digitali e a riaffermare il primato dei valori democratici. Questo orientamento, peraltro, riecheggia le riflessioni già espresse dalla Cancelliera tedesca Angela Merkel, la quale ha sottolineato l'importanza di un

Contestualmente inizia a palesarsi la necessità di arginare l'impatto sempre maggiore delle nuove tecnologie nell'area del diritto, impatto che ha scaricato le coordinate su cui si fondava l'esercizio tradizionale dei pubblici poteri a partire dal principio di territorialità fino alla nozione stessa di sovranità³¹.

3. La sfida della cybersecurity: protezione dei dati e normative nell'era delle violazioni informatiche

Sono enormi le quantità di dati³² che ogni giorno vengono generate e raccolte da organizzazioni pubbliche³³ e private. Elaborati, analizzati, condivisi e riutilizzati per estrarne valore prezioso, diventano sempre più spesso un bersaglio ambito per le intrusioni e le violazioni della sicurezza informatica. Per come si evince dal Rapporto 2024

sulla Sicurezza ICT solo in Italia (CLUSIT)³⁴ gli attacchi cibernetici sono in espansione. Confrontando i dati del 2019 con quelli del 2023 la crescita in termini numerici degli attacchi rilevati da fonti pubbliche è stata del 60% (da 1.667 a 2.779). Nel 2023 gli attacchi sono aumentati dell'11% a livello globale (ma in Italia sono aumentati ben del 65%). È indubbio che ci troviamo di fronte a un incremento esponenziale della superficie di attacco con impatti profondi, duraturi e sistemici su ogni aspetto politico, economico ma anche e soprattutto sociale. È difatti dall'uso improprio e malevolo di dati e in particolare di dati personali che si alimenta quella disparità informatica in cui i diritti fondamentali sono preda del dominio digitale. Così, attraverso una corposa produzione normativa sia il legislatore europeo che il legislatore nazionale³⁵

patto intergenerazionale che consenta di plasmare un futuro digitale all'insegna della sostenibilità e dell'equità. In tale prospettiva, la Conferenza sul Futuro dell'Europa rappresenta un'occasione cruciale per rinsaldare i legami tra le istituzioni comunitarie, i cittadini e la società civile, anche attraverso l'utilizzo di innovative piattaforme digitali.

31. DE ROSA 2021, p. 11. Si veda ancora GATTI 2019.

32. Come riportato nella Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regioni, *Una strategia europea per i dati*, COM(2020) 66, 12 febbraio 2020, 2, il volume dei dati prodotti a livello mondiale è in rapida crescita, dai 33 zettabyte del 2018 ai 175 zettabyte previsti nel 2025. È utile considerare anche che i dati e le informazioni aumentano ad una velocità vertiginosa tale da creare un ambiente saturo di dati, in tal senso GALETTA 2018, p. 327, riporta alcuni dati inerenti al tema dell'aumento del volume delle informazioni disponibili.

33. Sull'integrazione tra digitalizzazione e data protection si veda FAINI 2019.

34. Si veda il Rapporto Clusit 2024.

35. In un quadro di collaborazione europea e internazionale, nel 2013 nel nostro Paese è stata formulata una prima architettura della sicurezza cibernetica nazionale mediante il DPCM del 24 gennaio 2013 (c.d. Decreto Monti). Il DPCM ha delineato «l'architettura istituzionale deputata alla sicurezza nazionale [...] con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionale» assegnando a questo scopo compiti spesso strettamente complementari a vari attori istituzionali (Presidente del Consiglio dei ministri, Comitato Interministeriale per la Sicurezza della Repubblica, Dipartimento delle Informazioni per la Sicurezza, Nucleo per la Sicurezza Cibernetica) rendendo perciò indispensabile l'instaurarsi di numerose interazioni reciproche tra gli stessi. Il panorama normativo nazionale ha poi subito modifiche nel 2017 con l'emanazione di un nuovo DPCM (c.d. Decreto Gentiloni), che ha delineato i nuovi assetti organizzativi dell'architettura nazionale di cybersecurity e ha introdotto una Strategia nazionale in materia mediante l'adozione del nuovo Piano Nazionale²¹, che aggiorna i provvedimenti del dicembre 2013. Per il primo intervento di rango primario, invece, si è dovuto attendere il 2018, con l'emanazione del d.lgs. 65/2018 (c.d. d.lgs. NIS). Con questo atto l'Italia, in recepimento della Direttiva NIS, ha rafforzato il proprio quadro normativo in materia di cybersecurity attraverso l'istituzione del Perimetro di sicurezza nazionale cibernetica, oltre l'adozione di una Strategia nazionale di sicurezza cibernetica da parte del Presidente del Consiglio dei ministri. Al d.lgs. NIS ha fatto seguito il d.l. 21 settembre 2019, n. 105 che ha definito il Perimetro di sicurezza nazionale cibernetica al fine di garantire un elevato livello di sicurezza delle reti, dei sistemi e dei servizi informatici delle amministrazioni pubbliche nonché degli enti e degli operatori sia pubblici che privati. Sul piano del diritto, pertanto, si riscontra una continua evoluzione

pongono quale obiettivo principale l'idea di perseguire l'interesse comune europeo ad abitare una società protetta nella sua dimensione *onlife*³⁶ e più resiliente alle minacce cibernetiche. I legislatori nel dettare le norme in materia di protezione dei dati personali, dimostrano una spiccata consapevolezza dell'enorme portata assunta, negli ultimi decenni, dal fenomeno della circolazione dei dati che ha reso le informazioni personali "disponibili al pubblico su scala globale"³⁷.

In questa prospettiva, nel 2013 la *Cybersecurity Strategy*³⁸ definisce gli orientamenti generali al fine di rafforzare l'efficienza complessiva dell'Ue. La Strategia, nel delineare i principi su cui è fondato il *cyberspazio*, evidenzia *in primis* il valore dei diritti e delle libertà fondamentali, sottolineando il rapporto sinergico tra *cybersicurezza* e protezione dei dati personali. Nella medesima prospettiva, la Direttiva NIS³⁹, attuata in Italia solamente nel 2018, rappresenta il primo esempio di normativa orizzontale e, quindi, il primo tentativo di armonizzazione dei livelli di sicurezza dei sistemi informatici. Essa introduce l'obbligo a carico degli Stati membri di provvedere affinché determinati soggetti

(operatori di servizi essenziali e fornitori di servizi digitali) notifichino senza indebito ritardo all'autorità competente o al gruppo d'intervento per la sicurezza informatica gli incidenti che abbiano un impatto rilevante rispettivamente sulla continuità dei servizi essenziali prestati o sulla fornitura di un servizio digitale.

Sempre più urgente appare dunque identificare regole, metodologie e strumenti più appropriati e idonei a proteggere i dati da accessi non autorizzati e da attacchi malevoli⁴⁰. In tal senso interviene il Regolamento 2016/679/UE (GDPR) imponendo di trattare i dati personali in modo da garantirne un'adeguata sicurezza e riservatezza, integrità e disponibilità⁴¹ e per impedire l'accesso o l'utilizzo non autorizzato delle informazioni e dei sistemi impiegati per il loro trattamento. In tale contesto la cybersecurity si pone al centro di un ampio e diffuso dibattito sul piano tecnologico, giuridico e politico identificandosi come uno dei pilastri su cui viene (ri)edificato il sistema europeo di protezione dei dati personali⁴².

Costruire un ecosistema digitale sicuro richiede l'adozione di standard riconosciuti per garantire

della cornice normativa, a cui si aggiungono il d.l. 14 giugno 2021, n. 82 e alcuni specifici commi della l. 29 dicembre 2022, n. 197. Il d.l. 82/2021 mira a rafforzare le misure a tutela della sicurezza mediante l'istituzione dell'Agenzia per la cybersicurezza nazionale (ACN), il Comitato interministeriale per la cybersicurezza (CIC) e il Nucleo per la cybersicurezza, al quale è conferito il ruolo di coadiuvare il Presidente del Consiglio dei ministri in materia di prevenzione di eventuali crisi o attacchi cyber. L'ACN assume la responsabilità di tutelare la sicurezza nazionale, inclusa quella nello spazio cibernetico, e dispone di funzioni di coordinamento tra le altre Autorità competenti nel settore e di predisposizione della Strategia nazionale di cybersicurezza. Al CIC sono attribuite funzioni di sorveglianza sull'attuazione della suddetta Strategia e di supporto alle politiche della Presidenza del Consiglio dei ministri nell'ambito del Perimetro di sicurezza. Infine, al Nucleo per la cybersicurezza è conferito il ruolo di coadiuvare il Presidente del Consiglio dei ministri nella prevenzione di eventuali crisi o attacchi cyber. I commi da 899 a 902 della legge n. 197/2022 danno attuazione alla Strategia nazionale di cybersicurezza, formalmente adottata mediante DPCM in data 17 maggio 2022, e rendono effettivo il relativo piano di implementazione istituendo nel bilancio del Ministero dell'Economia e delle Finanze specifici fondi.

36. FLORIDI 2015; FLORIDI 2009.

37. Regolamento Generale sulla Protezione dei Dati (GDPR) - Considerando 6.

38. Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Strategia dell'Unione europea per la cybersicurezza: un cyberspazio aperto e sicuro*, Bruxelles, 7 febbraio 2013 [JOIN\(2013\) 1](#).

39. Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

40. FLOR 2019, p. 5.

41. V. PASSAGLIA 2016; PIZZETTI 2016, p. 9 ss. Sull'integrazione tra digitalizzazione e data protection si veda FAINI 2019.

42. FLOR 2019.

che le soluzioni tecniche utilizzate siano resilienti e che gli utenti possano fidarsi della protezione dei propri dati. Sarà il Regolamento UE 2019/881 (*Cybersecurity Act*)⁴³ a porre come obiettivo principale quello di rafforzare la resilienza dell'Unione agli attacchi informatici e favorire la c.d. “*security by design*” e il consolidamento di una *cybersecurity culture*⁴⁴ fin dagli stadi iniziali della progettazione o della realizzazione dei prodotti e dei servizi tecnologici, in cui sono compresi i dispositivi di consumo connessi alla rete e a quella sua parte c.d. IoT (*Internet of Things*).

Il Regolamento UE 2019/1150⁴⁵ rappresenta un fondamentale strumento normativo che si prefigge l'obiettivo di introdurre maggiore equità e trasparenza nelle relazioni contrattuali tra le piattaforme

digitali e gli utenti commerciali. Il succitato Regolamento inizia a considerare la crescente dipendenza delle imprese dagli intermediari digitali e a valutare le condizioni svantaggiose che in un rapporto sbilanciato possono derivare per i consumatori finali⁴⁶. In questa direzione la Commissione europea ha più volte sottolineato l'importanza di garantire l'indipendenza digitale dell'Unione europea da potenziali influenze di giurisdizioni straniere e nella comunicazione *Plasmare il futuro digitale dell'Europa 20*⁴⁷, evidenzia che le tecnologie digitali devono non solo contribuire al progresso dell'Europa migliorando la vita delle persone e la competitività delle imprese europee, ma anche rispettare i valori fondamentali su cui si basa l'Europa stessa. La Commissione, proprio al fine

43. Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Regolamento (UE) n. 526/2013 «regolamento sulla cibersicurezza». In *primis* il regolamento, da un lato, definisce genericamente la “cibersicurezza” come l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche; dall'altro lato, adotta una nozione omnicomprendensiva di “minaccia informatica”, intesa come una qualsiasi circostanza, evento o azione che potrebbe danneggiare, turbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone. In secondo luogo, il *Cybersecurity Act* vuole istituire un quadro europeo di certificazione al fine di migliorare il livello di cybersecurity in Europa, anche attraverso l'armonizzazione dei sistemi europei di certificazione della sicurezza informatica.

44. Riferimenti in tal senso si rinvencono anche nel report pubblicato da ENISA nel 2017: cfr. ENISA 2017, in cui si legge «Cybersecurity Culture (CSC) of Organizations refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people's behaviour with information technologies. [...] (T)echnologies cannot protect organisations if incorrectly integrated and utilised.» (p. 7 ss.). In un secondo report del 2019 ENISA riprende il difetto di una nozione universale di cybersecurity («there is no universally accepted definition of cybersecurity, with descriptions of the term varying across authors on multiple dimensions, including the nature of what is protected, from whom, and whether or not unintentional actions are included Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity»), concentrandosi su *human aspects of cybersecurity*, dal punto di vista “defending organisations”, e “socio-technical perspective”. Cfr. ENISA 2019, che parte dai risultati del report ENISA 2016.

45. Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio del 20 giugno 2019 che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online.

46. La proposta attuale si basa sulla constatazione che le grandi piattaforme digitali esercitano un controllo significativo sull'accesso ai mercati digitali, agendo come principali intermediari tra gli utenti finali e le imprese. Grazie alla loro posizione di dominio e alla capacità di profilare dettagliatamente gli utenti, tali piattaforme possono adottare pratiche commerciali che favoriscono la propria posizione a discapito della concorrenza leale. Al fine di promuovere un ambiente di mercato più equo e competitivo, la nuova proposta di regolamento identifica specifici “servizi digitali base” controllati da un numero limitato di grandi piattaforme. Questi servizi comprendono intermediazioni, social network, motori di ricerca e altri, mirando a garantire che le regole siano rispettate in modo da tutelare gli interessi degli utenti commerciali e dei consumatori finali. Si veda a tal proposito ALLEGRI 2021.

47. COMMISSIONE EUROPEA 2020.

di proteggere l'indipendenza digitale dell'Unione, propone di introdurre nuove regole volte a contrastare comportamenti e contenuti illeciti online, di definire chiaramente le responsabilità dei gestori dei flussi di informazioni e dati, e di aumentare la trasparenza nella gestione delle informazioni su Internet. La Direttiva NIS 2⁴⁸, proposta nel dicembre 2020 e entrata in vigore a gennaio 2023, insieme al Regolamento *Cyber Resilience Act* (CRA) rappresentano invece un passo significativo verso la creazione di principi comuni e regole di *policy* sulla cybersecurity per affrontare le crisi causate da diversi livelli di resilienza cibernetica tra gli Stati membri. Riconoscendo la dinamicità e la costante evoluzione delle minacce cibernetiche e la necessità di bilanciare le esigenze della sicurezza informatica, dell'innovazione tecnologica con il rispetto dei diritti dei cittadini sarà il Regolamento 2023/2841⁴⁹ a delineare una difesa comune basata su misure orientate ad una resilienza digitale⁵⁰ integrata e avanzata. Il Regolamento in vigore dal 1° gennaio 2024 stabilisce misure per un livello comune elevato di cibersecurity nelle istituzioni, negli organi e negli organismi dell'Unione ponendo quale obiettivo principale quello di proteggere i dati e la sovranità digitale degli Stati membri senza ostacolare l'innovazione e la competitività in un mercato digitale sempre più globale e dinamico.

Nonostante la corposa produzione normativa, ad oggi è ancora carente una lettura unitaria di

obblighi e doveri e questo determina una disparità di livelli di *cyber* resilienza tra gli Stati membri. Questo scenario inibisce la creazione di un *framework* di *cybersicurezza* coerente, uniforme e soprattutto la capacità di resistere alle pressioni di un mercato sempre più aperto e competitivo. Non è un caso che ad oggi Commissione europea e Agenzia Europea per la Sicurezza Informatica (ENISA) siano al centro di un dibattito sull'*European Cybersecurity Certification Scheme for Cloud Services* (EUCS)⁵¹. La nuova versione della bozza per la certificazione *cloud* non comprende gli stringenti requisiti di sovranità digitale che caratterizzavano la prima proposta avanzata in adesione al *Cybersecurity Act*⁵². Il progetto di schema di certificazione di sicurezza per i servizi di *cloud* (EUCS) inizialmente includeva requisiti di sovranità che avrebbero richiesto ai fornitori di servizi di *cloud* di localizzare i dati e le operazioni all'interno dell'Ue. In altre parole, i requisiti di sovranità avrebbero costretto i principali fornitori di *cloud* non Ue come AWS, Google e Microsoft a fare investimenti massicci in infrastrutture di data center locali dedicate, processi di conformità regolamentare e capacità di controllo sovrano per offrire servizi nell'Ue⁵³. Il progetto di schema EUCS più recente ha, pertanto, rimosso i requisiti di sovranità al fine di scongiurare il pericolo di limitare la concorrenza, aumentare i costi e frenare l'innovazione⁵⁴.

48. Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersecurity nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).

49. Regolamento (Ue, Euratom) 2023/2841 del Parlamento europeo e del Consiglio del 13 dicembre 2023 che stabilisce misure per un livello comune elevato di cibersecurity nelle istituzioni, negli organi e negli organismi dell'Unione.

50. Quando parliamo di resilienza digitale non parliamo di un ossimoro, ma di un profondo cambio di paradigma. La crisi pandemica, in particolare, ha messo in rilievo l'immagine di una tecnologia digitale frenetica, transitoria, a rapida obsolescenza, fonte di continua innovazione, ma anche in grado di permettere al sistema Paese di resistere, di affrontare l'impatto di eventi imprevedibili o addirittura impensabili.

51. Bozza di proposta dell'*European Cybersecurity Certification Scheme for Cloud Services* (EUCS).

52. In forza del Regolamento (UE) 2019/881, il quadro di certificazione di cybersecurity dell'Ue stabilisce la procedura per la creazione di schemi di certificazione di cybersecurity dell'Ue, che coprono i prodotti, i servizi e i processi ICT. Ogni schema specificherà uno o più livelli di assicurazione (basico, sostanziale o alto), in base al livello di rischio associato all'utilizzo previsto del prodotto, del servizio o del processo.

53. Si vedano a tal proposito gli annunci di alcuni dei principali fornitori di cloud non Ue: *AWS Digital Sovereignty*, *Microsoft Cloud for Sovereignty*.

54. CHEE 2024.

4. Sovranità digitale e cybersecurity: sinergia a tutela dei diritti nell'era delle crisi globali

Nella contemporanea società del rischio⁵⁵ il dibattito sul concetto di sovranità digitale ha come cornice un contesto particolarmente delicato segnato prima dalla pandemia⁵⁶ e a seguire dai conflitti bellici⁵⁷ che coinvolgono anche i paesi dell'Ue e che pongono enormi interrogativi sui possibili sviluppi in ottica *cyber*.

Le minacce cibernetiche rappresentano difatti un nemico sempre più evoluto e insidioso per l'esercizio dei diritti collettivi ed individuali e la fitta risposta normativa in materia di cybersecurity è prova e testimonianza della tensione esistente. Nondimeno, il concetto di sovranità digitale è ancora essenzialmente inteso come pratica politica discorsiva piuttosto che giuridica normativa⁵⁸ generando una situazione di frammentazione globale che esprime la crisi della rappresentazione unitaria del potere⁵⁹. La sovranità digitale, intesa come la capacità di gestire in modo autonomo le tecnologie digitali e le informazioni, rappresenta una sfida cruciale per la stabilità e la sicurezza geopolitica dell'Ue⁶⁰. In una società iperconnessa

ed interconnessa caratterizzata da forti legami transnazionali e interpretazioni pluraliste della democrazia è pertanto necessario e inevitabile un confronto più stretto tra i paesi membri.

La realizzazione di una visione unitaria a livello comunitario si scontra con criticità interne ai vari Stati, che ostacolano il raggiungimento di una posizione comune. Differenze di interessi, priorità e obiettivi specifici legati alla propria agenda politica, economica e sociale, inibiscono le esigenze di una gestione coordinata. Nel mentre, disparità economiche e di *status* sociale all'interno dei singoli Stati, che si manifestano anche nell'accesso alle tecnologie e alle competenze digitali, continuano a generare tensioni e conflitti che si ripercuotono sulla coesione sociale a vantaggio degli Stati e dei cittadini con maggiori risorse e competenze e a discapito di una visione di insieme. L'assenza di allineamento strategico si riflette inevitabilmente sulla capacità di definire standard, norme e regole condivise per una sovranità digitale che sembra diventare una vera e propria sfida.

Appare riduttivo affermare che la definizione delle modalità di trattamento e delle condizioni per il trasferimento transnazionale dei dati

55. BECK 2013.

56. L'*European Council on Foreign Relations* (ECFR) propone in un paper un nuovo concetto di Sovranità digitale intesa come la capacità di un Paese di governare le nuove tecnologie digitali e il loro impatto sulla società. L'organizzazione ne sottolinea la rilevanza, soprattutto dopo la pandemia di COVID-19, che ha dimostrato l'importanza fondamentale del digitale e dei dati per determinare il proprio destino, sia a livello personale che nazionale, in termini di resilienza economica e sanitaria. Inoltre, la crisi attuale spinge l'Europa a utilizzare in modo decisivo i dati come leva per rinnovare il proprio sistema produttivo e stimolare la ripresa economica. Si veda: *Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry*.

57. Si veda a tal proposito MEZZANOTTE 2022, in cui si evidenziano i pericoli della sovranità digitale di un Paese messa a rischio dagli attacchi hacker, che tendono ad intensificarsi durante i periodi di conflitto anche attraverso la diffusione di fake news e la creazione di deepfake. Sull'argomento si veda inoltre BERTONI 2019, p. 11. Sull'argomento si veda ancora di PIETROPAOLI 2019, in cui l'autore evidenzia come il concetto di cyberspazio sia destinato a cambiare la natura dei conflitti e quali danni sia possibile infliggere con un atto di guerra cibernetica. Ancora PIETROPAOLI 2023.

58. POHLE-THIEL 2020.

59. Si veda a tal proposito FERRARESE 2017. L'autrice sostiene che "Lo stato, inteso tipicamente come un soggetto unitario, quale era nella rappresentazione sovrana, nei vari regimi internazionali si rifrange in figure composte, come in un quadro cubista, dando luogo ad una situazione di prevalente "frammentazione" nello scenario internazionale, che riguarda sia le norme che l'autorità", facendo riferimento a BROUDE 2008.

60. Si veda a tal proposito ALÙ 2022, p. 253 in cui l'autore scrive che l'Europa aspira a conquistare la c.d. sovranità digitale, come obiettivo strategico di integrazione sovranazionale volto a realizzare un indispensabile riposizionamento geopolitico della propria centralità nella ridefinizione dei rapporti di forza esistenti su scala globale rispetto alle dinamiche conflittuali della predominante competizione tecnologica dualistica USA-Cina.

personali rappresentano l'espressione dell'esercizio di poteri sovrani da parte di uno Stato di diritto⁶¹ quando sono ancora molte le criticità riscontrabili nel caso in cui i dati vengono raccolti in un Paese e trattati in uno ospitante⁶². Quest'ultimo potrebbe, difatti, imporre le sue regolamentazioni, causando potenziali conflitti normativi a danno dei cittadini⁶³.

Parimenti, non è sufficiente limitare il potere pervasivo e intrusivo delle grandi multinazionali senza prevedere forme di contrasto al sovranismo digitale⁶⁴ e all'esercizio del suo potere di controllo⁶⁵ attraverso i dati degli individui che tradotti in profili, identificati tramite flussi di dati, degradano, citando Deleuze, a soggetti "dividuali"⁶⁶.

Se «un cellulare è un congegno di rintracciamento che fa anche telefonate»⁶⁷, è innegabile che

siano le élite economiche, tecnologiche e politiche a gestirne il controllo.

Un controllo tecno-sociale fondato sulla gestione degli algoritmi che sono gli elementi operativi dei dispositivi e basato sull'elaborazione dei dati degli algoritmi stessi che permette anche di prevedere comportamenti futuri grazie a modelli predittivi avanzati che consentono di classificare e profilare la vita degli individui⁶⁸ spingendoli nel cosiddetto "capitalismo della sorveglianza"⁶⁹.

Nessuna "microfisica" del potere, per riprendere Michel Foucault⁷⁰, potrebbe oggi prescindere dall'analisi dell'impatto dirompente del digitale sul nostro vivere, in privato e in pubblico, e sulla stessa dinamica democratica⁷¹.

Per frenare l'estensione del Panopticon digitale⁷², in cui la sorveglianza si fonde con il desiderio

61. ZENO-ZENCOVICH 2016.

62. Si veda a tal proposito il Provvedimento n. 112 del 30 marzo 2023 del Garante Privacy con cui l'Autorità ha disposto, con effetto immediato, la limitazione provvisoria del trattamento dei dati degli utenti italiani nei confronti di OpenAI società che gestisce la piattaforma di intelligenza artificiale ChatGPT per violazione delle norme a tutela della privacy. Si veda ancora il successivo comunicato stampa del 29 gennaio 2024 con cui il Garante notifica a OpenAI, l'atto di contestazione per aver violato la normativa in materia di protezione dei dati personali.

63. MANGIAMELI 2023; BERTOLA 2022.

64. Si veda a tal proposito ALPINI 2022. L'autrice cita l'esempio del d.l. n. 105 del 2019 e succ.ve modifiche, intitolato "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica" incentrato proprio sul concetto di sovranità nazionale e per questo criticato da una parte della dottrina quale espressione di sovranismo.

65. Si veda a tal proposito FROSINI 1968; RODOTÀ 1973. MANTELERO 2012, p. 135 ss.

66. Si veda a tal proposito SANTANIELLO 2022 in cui l'autore cita la Dichiarazione italiana dei diritti in Internet fortemente voluta da Stefano Rodotà e la recente *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale* elaborata dalla Commissione europea e da quest'ultima inviata al Parlamento europeo e al Consiglio il 26 gennaio 2022 per una sottoscrizione congiunta. Cita ancora la *Dichiarazione di Berlino sulla società digitale e su un governo digitale fondato sui valori* e la *Dichiarazione di Lisbona – Democrazia digitale con uno scopo* in cui si evidenzia la necessità di incanalare la trasformazione digitale nel solco dei valori della *good governance* europea.

67. ASSANGE 2013.

68. STRIKWERDA 2023.

69. RESTA 2019, p. 199 ss. Sul punto, cfr. SIMONCINI 2019. Si veda TALIA 2023, p. 517 in cui l'autore scrive che «il codice degli algoritmi di machine learning sta diventando sempre più il soggetto che stabilisce i termini in base ai quali viene vissuta la vita delle persone, non soltanto nello spazio digitale, ma anche nello spazio fisico della loro vita, eliminando così anche le ultime barriere che tra questi due spazi esistono e che sono destinate a essere abbattute del tutto».

70. FOUCAULT 1982.

71. FARINOSI 2011, pp. 180-189.

72. Il concetto di controllo è centrale nell'analisi del Panopticon, un'innovativa struttura carceraria concepita da Jeremy Bentham. Questo edificio, grazie alla sua peculiare architettura circolare che ruota attorno a una torre centrale, permette a un singolo sorvegliante di monitorare una moltitudine di detenuti. L'ingegno dell'architettura risiede nel fatto che i prigionieri, isolati in celle equidistanti, non possono vedere il sorvegliante, ma sono

di visibilità, creando un ciclo ininterrotto di controllo e auto-disciplina⁷³, è dunque necessario legare il concetto di sovranità (digitale) alla capacità di difendere i valori liberali e democratici.

Solo attraverso il rispetto dei principi e dei valori cardine posti a garanzia dei diritti fondamentali è difatti possibile scongiurare la pervasività del controllo e la manipolazione dei flussi informativi. Porre un freno alla violazione della

privacy e così alle limitazioni delle libertà⁷⁴ è l'unico antidoto contro pericolose derive autoritarie. Questo presuppone un processo politico-culturale⁷⁵ che inizi a guardare con favore alla costruzione di un democratico concetto di sovranità digitale in cui riconoscere il rispetto della gerarchia delle fonti di diritto internazionale⁷⁶ e l'esistenza di un costituzionalismo digitale⁷⁷ demandato a codificare i diritti digitali⁷⁸ rappresenta il primo passo per

costantemente indotti a credere di essere osservati. Tale percezione perpetua di sorveglianza invisibile induce nei detenuti un comportamento conforme, favorendo la loro riabilitazione attraverso l'interiorizzazione della disciplina. Michel Foucault ha ripreso e ampliato questa riflessione, applicando il principio del Panopticon a diverse istituzioni totali come il carcere, i manicomi, le fabbriche, le scuole, la famiglia. Nella sua opera *Sorvegliare e punire*, Foucault argomenta che i meccanismi di controllo e sorveglianza, seppur sottili e spesso impercettibili, permeano la società contemporanea, creando una standardizzazione comportamentale. La società, inconsapevolmente sorvegliata, è modellata da un sistema di premi e punizioni volto a promuovere un'omogeneità di pensiero e azione, facilitando il controllo sociale. Con l'avvento dell'era digitale, il Panopticon si è trasformato in un nuovo paradigma di sorveglianza virtuale in cui la distinzione tra sorvegliante e sorvegliato si dissolve: ciascuno è contemporaneamente osservatore e osservato. La condivisione incessante di esperienze, preferenze e dettagli personali costruisce una narrazione pubblica della nostra identità, esponendola a un pubblico potenzialmente illimitato. Questo nuovo modello di controllo digitale è caratterizzato dalla raccolta e analisi di dati personali da parte delle grandi piattaforme, che li utilizzano per profilazione e pubblicità mirata a discapito della privacy. Così, il Panopticon virtuale di Bentham si realizza nella Rete, dove la sorveglianza si fonde con il desiderio di visibilità, creando un ciclo ininterrotto di controllo e auto-disciplina. Si veda a tal proposito FOUCAULT 1976, pp. 21-22; STANZIONE 2020.

73. TALIA 2023.

74. CALIFANO 2016; si veda ancora COLAPIETRO 2018, p. 34, secondo cui la privacy «assume il carattere di “garanzia presupposto” dell'esercizio di altri diritti fondamentali, al fine di rendere possibile lo sviluppo della persona, l'esplicazione reale ed effettiva delle sue libertà».

75. SANTANIELLO 2021, p. 595.

76. In particolare, quelle di protezione generale dei diritti umani come la *Dichiarazione Universale dei Diritti Umani* approvata dall'Assemblea delle Nazioni Unite a Parigi il 10 dicembre 1948, la *Convenzione Unesco*, firmata a Londra nel 1945, la *Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, firmata a Roma il 4 novembre 1950.

77. POLLICINO 2023.

78. Si veda a tal proposito RESTA 2019, p. 222 in cui l'autore menziona il diritto a non essere oggetto di decisioni automatizzate; JØRGENSEN 2019; CATH 2018. Nel panorama nazionale Stefano Rodotà, in occasione del III Internet Governance Forum, avanzò una proposta di modifica costituzionale formulando un articolo 21-*bis* in base al quale «Tutti hanno eguale diritto di accedere alla rete Internet, in condizione di parità, con modalità tecnologicamente adeguate e che rimuovano ogni ostacolo di ordine economico e sociale». L'art. 21-*bis*, tuttavia, non è stato assunto come dettame costituzionale ma la proposta di Rodotà, nel luglio 2015, è confluita nella *Dichiarazione dei diritti di Internet*, che riconosce come Internet abbia «contribuito in maniera decisiva a ridefinire lo spazio pubblico e privato, a strutturare i rapporti tra le persone e tra queste e le Istituzioni. Internet ha cancellato confini e ha costruito modalità nuove di produzione e utilizzazione della conoscenza. Ha ampliato le possibilità di intervento diretto delle persone nella sfera pubblica. Ha modificato l'organizzazione del lavoro. Ha consentito lo sviluppo di una società più aperta e libera». Internet, secondo questa linea di indirizzo, deve essere considerata come una risorsa globale che risponde al criterio della universalità e proprio per questo l'articolo 2 sancisce «l'accesso ad Internet come diritto fondamentale della persona e condizione per il suo pieno sviluppo

democratizzare la sovranità digitale e spingere gli individui ad autodeterminarsi⁷⁹ e ad esercitare il diritto di controllo sui propri dati⁸⁰.

Creare dunque un nuovo spazio di esercizio della sovranità, che trascende i confini geografici e si estende all'ambito digitale, permettendo ai cittadini di esercitare il loro potere e di partecipare attivamente alla vita politica in modo più efficace e inclusivo⁸¹. Rievocando l'idea di Rousseau, in una moderna democrazia, la sovranità appartiene al popolo e non ad un monarca⁸². In tal senso anche la sovranità digitale non può che elevarsi a spazio di esercizio e di azione della sovranità del popolo cui è demandata l'autorità di esercizio⁸³ dei propri diritti e interessi personali.

5. Conclusioni

La cybersecurity non può esaurirsi a un mero apparato tecnico normativo, ma deve elevarsi a baluardo della sovranità digitale, intesa non come sterile rivendicazione di potere, bensì come presidio dei diritti e delle libertà dei cittadini nel perimetro del *cyberspazio*. I due concetti trovano la loro più autentica espressione in una visione d'insieme che li colloca in una relazione di reciproca implicazione. Solo attraverso tale sinergia, ove sicurezza e

sovranità si compenetrano in un nesso inscindibile, è dato ipotizzare un *corpus* normativo unitario che sorregga e informi l'azione statale sulla base dei condivisi principi democratici.

La cybersecurity diviene condizione di possibilità per l'esercizio di una sovranità che, lungi dal rimanere ancorata a confini geografici, si proietta nella dimensione digitale, rendendosi garante dell'autodeterminazione informativa dei singoli e della comunità. Contestualmente, la sovranità digitale, non risolvibile in un mero atto di forza, trova la sua legittimazione ultima nella capacità di assicurare la sicurezza dei dati e delle informazioni, sottraendoli a ingerenze indebite e a utilizzi distortivi. Due concetti fondamentali, per concludere, da intendersi come espressione di una volontà politica che si fa interprete di istanze di tutela e di promozione della persona umana, anche e soprattutto nel suo rapporto con le nuove tecnologie. L'auspicio è che si possa giungere a un cambio epocale di paradigma sulla base di un approccio radicale e innovativo in cui cybersecurity e sovranità digitale, cariche di una valenza etica, si pongano a tutela di una democrazia non ancorata a schemi obsoleti delineando il passaggio dall'*Internet of thing* al *Right over thing*.

Riferimenti bibliografici

- M.R. ALLEGRI (2021), *Il futuro digitale dell'Unione europea: nuove categorie di intermediari digitali, nuove forme di responsabilità*, in "Rivista italiana di informatica e diritto", 2021, n. 2
- A. ALPINI (2022), *La sovranità digitale europea*, in "Tigor. Rivista di scienze della comunicazione e di argomentazione giuridica", 2022, n. 2
- A. ALÙ (2022), *La Governance di Internet oltre gli Stati? Gli inediti tratti del futuro ecosistema digitale*, in "Rivista italiana di informatica e diritto", 2022, n. 1
- A.C. AMATO MANGIAMELI, M.N. CAMPAGNOLI (2020), *Strategie digitali. #diritto_educazione_tecnologia*, Giappichelli, 2020

individuale e sociale». L'articolo continua prevedendo che «Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale» Sull'argomento si veda SPAGNUOLO-SORRENTINO 2021, pp. 276-286.

79. MANGIAMELI 2011.

80. Il rispetto dei principi di trasparenza, di non esclusività della decisione automatizzata e del consenso, sanciti dagli artt. 12, 13, 14, 15 e 22 del GDPR rappresentano il presupposto giuridico del controllo sui propri dati.

81. Si veda a tal proposito SANTANIELLO 2022.

82. NOONE 1970, pp. 696-708.

83. COUTURE-TOUPIN 2019; POHLE-THIEL 2020.

- J. ASSANGE (2013), *Internet è il nemico. Conversazione con Jacob Appelbaum, Andy Müller-Maguhn e Jérémie Zimmermann*, Feltrinelli, 2013
- S. AUTOLITANO, A. PAWLOWSKA (2021), *Europe's Quest for Digital Sovereignty: Gaia X as a Case Study*, IAI Papers, 2021, n. 14
- J.P. BARLOW (1996), *Dichiarazione di indipendenza del Cyberspazio*, 1996
- U. BECK (2013), *La società del rischio. Verso una seconda modernità*, Carocci, 2013
- V. BERTOLA (2022), *La sovranità digitale e il futuro di Internet*, in "Rivista italiana di informatica e diritto", fascicolo monografico a cura di L. Abba, A. Lazzaroni, M. Pietrangelo, 2022, n. 1
- F. BERTONI (2019), *Deepfake, ovvero Manipola et impera. Un'analisi sulle cause, gli effetti e gli strumenti per la sicurezza nazionale, nell'ambito dell'utilizzo malevolo dell'intelligenza artificiale ai fini di disinformazione e propaganda*, in "Cyberspazio e diritto", 2019, n. 1-2
- B. BRIGHI, P.G. CHIARA (2021), *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in "federalismi.it", 2021, n. 21
- T. BROUDE (2008), *Fragmentation(s) of International Law: On Normative Integration as Authority Allocation*, in T. Broude, Y. Shany (eds.), "The Shifting Allocation of Authority in International Law: Considering Sovereignty, Supremacy, and Subsidiarity", Hart Publishing, 2008
- L. CALIFANO (2016), *Privacy: affermazione e pratica di un diritto fondamentale*, Editoriale Scientifica, 2016
- A. CASSESE (2006), *Diritto internazionale*, a cura di P. Gaeta, il Mulino, 2006
- C. CATH (2018), *Governing artificial intelligence: ethical, legal and technical opportunities and challenges*, in "Philosophical Transactions of the Royal Society A", 2018
- F.Y. CHEE (2024), *EU drops sovereignty requirements in cybersecurity certification scheme, document shows*, Reuters, 2024.
- C. COLAPIETRO (2018), *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello. Il Regolamento UE 2016/679 parametro di legittimità della complessiva normativa sulla privacy*, Editoriale Scientifica, 2018
- COMMISSIONE EUROPEA (2020), *Plasmare il futuro digitale dell'Europa*, 2020
- S. COUTURE, S. TOUPIN (2019), *What does the notion of "sovereignty" mean when referring to the digital?*, in "New Media & Society", vol. 21, 2019, n. 10
- M. CUNIBERTI (a cura di) (2008), *Nuove tecnologie e libertà della comunicazione. Profili costituzionali e pubblicistici*, Giuffrè, 2008
- J.-P. DARNIS (2021), *L'Unione europea tra autonomia strategica e sovranità tecnologica: problemi e opportunità*, IAI Papers, 2021, n. 19
- P. DE ROSA (2021), *Concetto di Stato e nuove tecnologie. Quale ruolo per lo Stato nello spazio digitale?*, in "Media Laws", 2021, n. 1
- ENISA - EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (2019), *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*, 2019
- ENISA - EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (2017), *Cyber Security Culture in organisations*, 2017
- ENISA - EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (2016), *Definition of Cybersecurity: Gaps and overlaps in standardization*, 2016

- M.S. ESPOSITO (2019), *Trattamento dei dati personali e rischi correlati, nel prisma dei diritti e delle libertà fondamentali*, in “Il Diritto dell’Informazione e dell’Informatica”, 2019, n. 4-5
- M. FARINOSI (2011), *Beyond the panopticon framework: Privacy, control and user generated content*, in A. Esposito, A.M. Esposito, R. Martone et al. (eds.), “Toward Autonomous, Adaptive, and Context-Aware Multimodal Interfaces. Theoretical and Practical Issues”, Springer, 2011
- M.R. FERRARESE (2017), *Il diritto internazionale come scenario di ridefinizione della sovranità degli Stati*, in “Stato e mercato”, 2017, n. 109
- F. FAINI (2019), *Il volto dell’amministrazione digitale nel quadro della rinnovata fisionomia dei diritti in rete*, in “Il diritto dell’informazione e dell’informatica”, 2019, n. 4-5
- F. FAINI (2019-A), *Diritto all’esistenza digitale*, in “BioLaw Journal – Rivista di BioDiritto”, 2019, n. 3
- G. FINOCCHIARO (2022), *La sovranità digitale*, in “Diritto pubblico”, 2022, n. 3
- G. FINOCCHIARO (2014), *La protezione dei dati personali e la tutela dell’identità*, in G. Finocchiaro, F. Del-fini (a cura di), “Diritto dell’informatica”, UTET, 2014
- R. FLOR (2019), *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, in “Diritto di internet”, 2019, n. 3
- L. FLORIDI (2015), *The Onlife Manifesto*, Springer, 2015
- L. FLORIDI (2009), *Infosfera. Etica e filosofia nell’età dell’informazione*, Giappichelli, 2009
- C. FORMENTI (2008), *Cybersoviet. Utopie postdemocratiche e nuovi media*, Raffaello Cortina Editore, 2008
- M. FOUCAULT (1982), *Microfisica del potere: interventi politici*, vol. 90, Einaudi, 1982
- M. FOUCAULT (1976), *Sorvegliare e punire. Nascita della prigione*, Einaudi, 1976
- P.W. FRANZESE (2009), *Sovereignty in Cyberspace: Can It Exist?*, in “The Air Force Law Review”, vol. 64, 2009
- V. FROSINI (1968), *Cibernetica, diritto e società*, Edizioni di Comunità, 1968
- D.-U. GALETTA (2018), *La Pubblica Amministrazione nell’era delle ICT: sportello digitale unico e Intelligenza Artificiale al servizio della trasparenza e dei cittadini?*, in “Ciberspazio e diritto”, 2018, n. 3
- A. GATTI (2019), *Istituzioni e anarchia nella rete. I paradigmi tradizionali della sovranità alla prova di internet*, in “Il diritto dell’informazione e dell’informatica”, 2019, n. 3
- D. HARVEY (2006), *La guerra perpetua. Analisi del nuovo imperialismo*, Il Saggiatore, 2006
- P. HUMMEL, M. BRAUN, M. TRETTER, P. DABROCK (2021), *Data sovereignty: A review*, in “Big Data & Society”, vol. 8, 2021, n. 1
- R.F. JØRGENSEN (ed.) (2019), *Human Rights in the Age of Platforms*, MIT Press, 2019
- T. MADIEGA (2020), *Digital Sovereignty for Europe*, European Parliamentary Research Service, PE 651.992, July 2020
- S. MANGIAMELI (2023), *La sovranità digitale*, in “Dirittifondamentali.it”, 2023, n. 3
- S. MANGIAMELI (2023-A), *La sovranità digitale*, in A.C. Amato Mangiameli, G. Saraceni (a cura di), “Cento e una voce di informatica giuridica”, Giappichelli, 2023
- S. MANGIAMELI (2011), *Autodeterminazione: diritto di spessore costituzionale?*, in C. Navarini (a cura di), “Autonomia e autodeterminazione. Profili etici, bioetici e giuridici”, Editori Riuniti, 2011
- A. MANTELERO (2012), *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in “Il diritto dell’informazione e dell’informatica”, 2012

- L. MARTINO (2018), *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in "Politica & società", 2018, n. 1
- M. MEZZANOTTE (2022), *Fake news, deepfake e sovranità digitale nei periodi bellici*, in "federalismi.it", 2022, n. 33
- L. MOEREL, P. TIMMERS (2021), *Reflections on Digital Sovereignty*, in "EU Cyber Direct, Research", Focus series, 2021
- J.B. NOONE (1970), *The Social Contract and the Idea of Sovereignty in Rousseau*, in "The Journal of Politics", vol. 32, 1970, n. 3
- M. OROFINO (2018), *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in "MediaLaws", 2018, n. 2
- P. PASSAGLIA (2016), *Privacy e nuove tecnologie, un rapporto difficile. Il caso emblematico dei social media, tra regole generali e ricerca di una specificità*, in "ConsultaOnline", 2016, n. 3
- S. PIETROPAOLI (2023), *Un altro modo di fare la guerra. La cyberwar come problema giuridico*, in "Ars interpretandi", 2023, n. 1
- S. PIETROPAOLI (2019), *Cyberspazio. Ultima frontiera dell'inimicizia? Guerre, nemici e pirati nel tempo della rivoluzione digitale*, in "Rivista di filosofia del diritto", 2019, n. 2
- F. PIZZETTI (2016), *Privacy e il diritto europeo alla protezione dei dati personali*, vol. II, *Il Regolamento europeo 2016/679*, Giappichelli, 2016
- J. POHLE, T. THIEL (2020), *Digital sovereignty*, in "Internet Policy Review", vol. 9, 2020, n. 4
- O. POLLICINO (2023), *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in "Quaderni costituzionali", 2023, n. 3
- O. POLLICINO, E. BERTOLINI, V. LUBELLO (a cura di) (2013), *Internet: regole e tutela dei diritti fondamentali*, Aracne, 2013
- G. RESTA (2019), *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in "Politica del diritto", 2019, n. 2
- S. RODOTÀ (2006), *Tecnologie e diritti*, il Mulino, 2006
- S. RODOTÀ (1973), *Elaboratori elettronici e controllo sociale*, il Mulino, 1973
- M. SANTANIELLO (2022), *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, in "Rivista italiana di informatica e diritto", 2022, n. 1
- M. SANTANIELLO (2021), *La regolazione delle piattaforme e il principio della sovranità digitale*, in "Rivista di Digital Politics", 2021, n. 3
- F. SERINI (2023), *La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersecurity. Alcune considerazioni alla luce delle discipline europea e italiana*, in "Rivista italiana di informatica e diritto", 2023, n. 2
- A. SIMONCINI (2019), *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in "BioLaw Journal – Rivista di BioDiritto", 2019, n. 1
- A. SIMONCINI (2017), *Sovranità e potere nell'era digitale*, in T.E. Frosini, O. Pollicino, E. Apa, M. Bassini (a cura di), "Diritti e libertà in Internet", Mondadori Education, 2017
- A. SIMONCINI, E. CREMONA (2022), *La AI fra pubblico e privato*, in "DPCE Online", 2022, n. 1
- A.F. SPAGNUOLO, E. SORRENTINO (2021), *Alcune riflessioni in materia di trasformazione digitale come misura di semplificazione*, in "federalismi.it", 2021, n. 8

- P. STANZIONE (2020), Intervento al Security Summit 2020, sessione “La sovranità tecnologica e digitale dell’Unione Europea: il difficile ruolo di mediazione con gli over the top e i rapporti con gli USA”, 12 novembre 2020
- L. STRIKWERDA (2023), Predictive identification als een moreel ondoor-zichtig panopticon, in “PROCES”, 2023, n. 3
- D. TALIA (2023), *Il potere disciplinare della governamentalità digitale*, in “Rivista di Digital Politics” 2023, n. 3
- P.A. WALKER (2015), Law of the Horse to Law of the Submarine: The Future of State Behavior in Cyberspace, in M. Maybaum, A.M. Osula, L. Lindstrom (eds.), “Architectures in Cyberspace”, 7th International Conference on Cyber Conflict, 2015
- V. ZENO-ZENCOVICH (2016), *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in G. Resta, V. Zeno-Zencovich (a cura di), “La protezione transnazionale dei dati personali. Dai ‘safe harbour principles’ al ‘privacy shield’”, RomaTrE-Press, 2016
- S. ZUBOFF (2019), *Il capitalismo della sorveglianza. Il futuro dell’umanità nell’era dei nuovi poteri*, Luiss University Press, 2019



**RIVISTA ITALIANA DI
INFORMATICA E DIRITTO**

PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0199 • articolo non sottoposto a peer review • pubblicato in anteprima il 23 dic. 2024
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale 

OSSERVATORIO SU

Intelligenza Artificiale e diritto

coordinato da Giancarlo Taddei Elmi

GIANCARLO TADDEI ELMI - SOFIA MARCHIAFAVA

Sviluppi recenti in tema di Intelligenza Artificiale e diritto

Una rassegna di legislazione, giurisprudenza e dottrina

maggio-ottobre 2024

G. Taddei Elmi è associato emerito del CNR presso l'Istituto di Informatica Giuridica e Sistemi Giudiziari di Firenze
S. Marchiafava è avvocato cassazionista, LLM in Comparative Law, docente del Master di II livello in Informatica
giuridica, nuove tecnologie e diritto dell'informatica presso Sapienza – Università di Roma

A. NORMATIVA

1. Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regolamento sull'intelligenza artificiale)

Il Regolamento (UE) 2024/1689 sull'intelligenza artificiale (d'ora in poi Regolamento sull'IA o AI Act), definitivamente approvato il 13 giugno 2024, è stato pubblicato il 12 luglio 2024 sulla [Gazzetta ufficiale dell'Unione europea](#) ed è entrato in vigore il ventesimo giorno successivo (1° agosto 2024).

Con i suoi 180 considerando, 113 articoli e 13 allegati, il Regolamento sull'IA sarà complessivamente applicabile e obbligatorio per tutti gli Stati membri a decorrere dal 2 agosto 2026. Alcune disposizioni saranno applicabili secondo una diversa tempistica specificamente prevista dallo stesso Regolamento all'art. 113, in particolare:

a) i Capi I (Disposizioni generali) e II (Pratiche di IA vietate) si applicheranno già a decorrere dal 2 febbraio 2025;

b) il Capo III, Sezione 4 (Autorità di notifica e organismi notificati), il Capo V (Modelli di IA per finalità generali), il Capo VII (Governance), il Capo XII (Sanzioni) e l'art. 78 (Riservatezza) si applicheranno a partire dal 2 agosto 2025, ad eccezione dell'art. 101 (Sanzioni pecuniarie per i fornitori di modelli di IA per finalità generali);

c) l'art. 6, paragrafo 1, in relazione ai criteri di classificazione per i sistemi di IA ad alto rischio e ai corrispondenti obblighi si applicheranno a decorrere dal 2 agosto 2027.

Dunque a livello nazionale gli Stati membri hanno tempo fino al 2 agosto 2025 per istituire le autorità nazionali competenti, che controlleranno l'applicazione delle norme per i sistemi di IA e svolgeranno attività di vigilanza del mercato; a livello europeo, è l'Ufficio per l'IA della Commissione europea a rivestire un ruolo fondamentale per l'attuazione del Regolamento. Svolgono rilevanti compiti consultivi il Comitato europeo per l'IA (composto da rappresentanti degli Stati membri), il Forum consultivo (portatori di interessi, tra cui l'industria, le start-up, le PMI, la società civile e il mondo accademico) e il Gruppo di esperti scientifici indipendenti (esperti selezionati dalla Commissione europea sulla base di competenze scientifiche o tecniche aggiornate nel settore dell'IA).

Per le imprese che non rispetteranno il Regolamento europeo sull'IA sono previste sanzioni pecuniarie: fino al 7 % del fatturato annuo mondiale in caso di non conformità al divieto delle pratiche di IA di cui all'art. 5 e fino al 3 % per le violazioni di alcuni specifici obblighi, tra questi, ad esempio, gli obblighi dei fornitori dei sistemi di IA ad alto rischio di cui all'art. 16 e fino all'1 % per la fornitura di informazioni inesatte (cfr. art. 99).

In attesa della complessiva applicazione della normativa europea, secondo i suddetti termini sanciti dall'art. 113 del Regolamento sull'IA, la Commissione europea ha previsto il Patto per l'IA per orientare gli sviluppatori di IA all'adozione volontaria degli obblighi fondamentali della regolamentazione.

Il 25 settembre 2024 la Commissione europea ha annunciato che almeno cento imprese hanno firmato tale Patto e i relativi impegni volontari finalizzati a una anticipata applicazione dei principi e regole del Regolamento sull'IA. In tale contesto sono previste diverse iniziative anche di formazione e su alcuni aspetti dell'AI Act e scambio di buone pratiche.

1.1. Regolamento europeo sull'intelligenza artificiale e protezione dei dati

1.1.a. European Data Protection Board (EDPB): dichiarazione n. 3/2024

A seguito della pubblicazione del Regolamento sull'IA, il Comitato europeo per la protezione dei dati (*European Data Protection Board* - EDPB) ha adottato, il successivo 16 luglio 2024, la dichiarazione n. 3/2024 a proposito del ruolo delle autorità per la protezione dei dati nell'ambito della disciplina giuridica sull'IA.

In particolare l'EDPB ha definito i rapporti tra il Regolamento europeo sull'IA e la normativa sulla protezione dei dati personali, in particolare il Regolamento (UE) n. 2016/679 (GDPR), il Regolamento (UE) 2018/1725 (EUDPR), la Direttiva (UE) 2016/680 (LED) e la direttiva 2002/58/CE, sottolineando che si tratta di strumenti legislativi complementari, come peraltro si evince dall'art. 2, paragrafo 7, dello stesso Regolamento sull'IA a norma del quale «Il diritto dell'Unione in materia di protezione dei dati personali, della vita privata e della riservatezza delle comunicazioni si applica ai dati personali trattati in relazione ai diritti e agli obblighi stabiliti dal presente regolamento. Il presente regolamento lascia impregiudicati il regolamento (UE) 2016/679 o (UE) 2018/1725 o la direttiva 2002/58/CE o (UE) 2016/680, fatti salvi l'articolo 10, paragrafo 5, e l'articolo 59 del presente regolamento».

Dopo avere evidenziato la stretta relazione tra le suddette normative, l'EDPB ha rilevato le competenze ed esperienze acquisite dalle autorità nazionali per la protezione dei dati personali, raccomandando di tenerne conto anche ai fini dell'individuazione delle autorità nazionali che dovranno vigilare negli Stati membri sull'applicazione del Regolamento sull'IA.

D'altra parte, ai sensi dell'art. 74, paragrafo 8, del Regolamento sull'IA, nella misura in cui i sistemi di IA ad alto rischio sono utilizzati a fini di attività di contrasto, gestione delle frontiere, giustizia e democrazia, gli Stati membri designano come autorità di vigilanza del mercato ai fini dello stesso Regolamento sull'IA le autorità di controllo competenti per la protezione dei dati a norma del regolamento (UE) 2016/679 o della direttiva (UE) 2016/680.

L'EDPB ha poi auspicato una stretta collaborazione tra le autorità a livello europeo e nazionale, in particolare tra l'Ufficio per l'IA e i garanti nazionali per la protezione dei dati.

Sul rapporto tra il Regolamento (UE) 2024/1689 (AI Act) e il Reg. (UE) n. 2016/679 (GDPR) si segnala l'articolo di Falletta-Marsano¹.

1.1.b. Garante italiano per la protezione dei dati personali: Web scraping ed intelligenza artificiale generativa - nota informativa e possibili azioni di contrasto

Molteplici sono i rischi per i diritti e le libertà connessi all'uso delle tecnologie di riconoscimento facciale e Web scraping, come in diverse occasioni è stato precisato anche in relazione alla disciplina giuridica dettata dal Regolamento (UE) 2016/679 sulla protezione dei dati personali.

Da ultimo, il Garante italiano per la protezione dei dati personali ha fornito il 20 maggio 2024 rilevanti indicazioni nel documento intitolato «Web scraping ed intelligenza artificiale generativa: nota informativa e possibili azioni di contrasto» (Provvedimento n. 329, GU Serie Generale n. 132, 7 giugno 2024).

Tali indicazioni riguardano il fenomeno della raccolta massiva di dati personali dal Web per finalità di addestramento dei modelli di intelligenza artificiale generativa e stabiliscono alcune possibili azioni di contrasto che i gestori di siti Internet e di piattaforme online, sia pubblici che privati, operanti in Italia, quali titolari del trattamento dei dati personali oggetto di pubblicazione, potrebbero adottare (Creazione di aree riservate, intervento sui bot, ecc.).

1. FALLETTA-MARSANO 2024.

1.1.c. G7 Privacy Italia 2024 - La privacy nell'era dei dati

In occasione della IV edizione G7 dei Garanti privacy tenutosi a Roma dal 9 all'11 ottobre 2024, coordinato quest'anno dal Garante italiano, è stata ribadita l'importanza del ruolo delle Autorità di protezione dei dati personali nella governance dell'IA che nell'Unione europea è in corso di realizzazione a seguito dell'entrata in vigore del Regolamento (UE) 2024/1689. In proposito è stato sottolineato che l'IA si alimenta con i dati personali, i Garanti privacy hanno una consolidata esperienza in numerosi settori (sanità, lavoro, ecc.) proprio sulla protezione dei dati e rivestono un ruolo che assicura la necessaria indipendenza e neutralità.

In conclusione sono state approvate la dichiarazioni su IA e minori ("Statement on AI and Children") nonché quella sul ruolo delle Autorità di protezione dei dati nel promuovere IA affidabile ("Statement on the Role of Data Protection Authorities in Fostering Trustworthy AI").

2. Iniziative legislative in Italia

2.1. Disegno di legge "Disposizioni e delega al Governo in materia di intelligenza artificiale" approvato il 23 aprile 2024

Il Consiglio dei ministri n. 78 del 23 aprile 2024 ha deliberato il disegno di legge "Disposizioni e delega al Governo in materia di intelligenza artificiale".

L'iter di approvazione ha preso l'avvio con la [presentazione del citato disegno di legge](#) il 20 maggio 2024 al Senato, A.S. 1146.

Il testo, suddiviso in sei Capi e costituito da 26 articoli, disciplina l'uso dell'IA con riferimento a diversi settori: sanità (art. 7-9), lavoro (art. 10-11), professioni intellettuali (art. 12), pubblica amministrazione (art. 13), attività giudiziaria (art. 14), cybersicurezza (art. 16). Inoltre, nell'ambito della strategia nazionale sull'IA e delle azioni di promozione (art. 17-22), il disegno di legge prevede investimenti (art. 21), la tutela del diritto d'autore con riguardo alle opere generate con l'ausilio dell'IA (art. 24), e alcune modifiche al codice di procedura civile (art. 15) e penale (art. 25) (cfr. [Focus: Analisi del quadro normativo in materia di Intelligenza artificiale](#), Presidenza del Consiglio dei ministri, Dipartimento per il programma di Governo). Qui di seguito l'impianto del disegno di legge, leggermente modificato rispetto alla bozza riportata nel precedente aggiornamento con l'aggiunta del Capo VI e dell'art. 26:

Capo I Principi e finalità

- Art. 1 Finalità e ambito di applicazione
- Art. 2 Definizioni
- Art. 3 Principi generali
- Art. 4 Principi in materia di informazione e di riservatezza dei dati personali
- Art. 5 Principi in materia di sviluppo economico
- Art. 6 Disposizioni in materia di sicurezza e difesa nazionale

Capo II Disposizioni di settore

- Art. 7 Uso dell'intelligenza artificiale in ambito sanitario e di disabilità
- Art. 8 Ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitari
- Art. 9 Disposizioni in materia di fascicolo sanitario elettronico, sistemi di sorveglianza nel settore sanitario e governo della sanità digitale
- Art. 10 Disposizioni sull'uso dell'intelligenza artificiale in materia di lavoro
- Art. 11 Osservatorio sull'adozione di sistemi di intelligenza artificiale nel mondo del lavoro
- Art. 12 Disposizioni in materia di professioni intellettuali
- Art. 13 Uso dell'intelligenza artificiale nella pubblica amministrazione
- Art. 14 Uso dell'intelligenza artificiale nell'attività giudiziaria
- Art. 15 Modifiche al codice di procedura civile

Art. 16 Uso dell'intelligenza artificiale per il rafforzamento della cybersicurezza nazionale

Capo III Strategia nazionale, Autorità nazionali e azioni di promozione

Art. 17 Strategia nazionale per l'intelligenza artificiale

Art. 18 Autorità nazionali per l'intelligenza artificiale

Art. 19 Applicazione sperimentale dell'intelligenza artificiale ai servizi forniti dal Ministero degli affari esteri e della cooperazione internazionale

Art. 20 Misure di sostegno ai giovani e allo sport

Art. 21 Investimenti nei settori dell'intelligenza artificiale, della cybersicurezza e del calcolo quantistico

Art. 22 Deleghe al Governo in materia di intelligenza artificiale

Capo IV Disposizioni a tutela degli utenti e in materia di diritto d'autore

Art. 23 Identificazione dei contenuti testuali, fotografici, audiovisivi e radiofonici, prodotti da sistemi di intelligenza artificiale

Art. 24 Tutela del diritto d'autore delle opere generate con l'ausilio dell'intelligenza artificiale

Capo V Disposizioni penali

Art. 25 Modifiche al codice penale e ad ulteriori disposizioni penali)

Capo VI Disposizioni finanziarie

Art. 26 Clausola di invarianza finanziaria

2.1.a. Parere favorevole del Garante per la protezione dei dati personali sullo schema di disegno di legge governativo sull'IA, recante anche delega legislativa per l'adeguamento al Regolamento Ue sull'Intelligenza Artificiale

Il 2 agosto 2023 il Garante per la protezione dei dati personali ha espresso il proprio [parere favorevole](#) al testo del suddetto disegno di legge chiedendo al Governo alcune integrazioni per garantire una maggiore tutela dei dati personali dei cittadini (Registro dei provvedimenti n. 477 del 2 agosto 2024).

In particolare il Garante ha chiesto di precisare che i trattamenti di dati personali effettuati attraverso i sistemi di IA devono rispettare la normativa privacy nazionale ed europea. Inoltre, il testo del disegno di legge dovrà essere integrato con uno specifico riferimento a sistemi adeguati di verifica dell'età (c.d. *age verification*) in grado di garantire limitazioni o divieti all'uso dei sistemi di IA da parte dei minori.

I sistemi di IA in ambito sanitario ad alto rischio dovranno indicare specifiche limitazioni per l'utilizzo dei dati (conservazione, divieto di trasmissione, trasferimento o comunicazione) e la preferenza per l'uso di dati sintetici o anonimi. Inoltre è stato richiesto di indicare il Garante per la protezione dei dati personali quale Autorità competente per i sistemi di IA ad alto rischio utilizzati, ad esempio, per le attività di contrasto, identificazione biometrica remota, riconoscimento delle emozioni, gestione delle frontiere, amministrazione della giustizia e processi democratici. Il Garante ha altresì evidenziato l'opportunità di prevedere, tra i criteri di delega, anche un suo adeguato coinvolgimento nella realizzazione degli spazi di sperimentazione normativa (nelle forme previste dall'art. 57 dell'AI Act).

3. Iniziative internazionali

3.1. Consiglio d'Europa: Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225)

Il 5 settembre 2024, a Vilnius, la Commissione europea ha sottoscritto la [Convenzione quadro del Consiglio d'Europa su Intelligenza artificiale, Diritti umani, Democrazia e Stato di diritto](#).

In linea con il Regolamento sull'IA, la Convenzione quadro è un primo accordo internazionale giuridicamente vincolante che impone agli Stati firmatari di adottare o mantenere misure adeguate per

identificare, verificare, prevenire e mitigare i rischi dei sistemi di IA in relazione ai diritti umani, la democrazia e lo Stato di diritto.

Articolata in 8 Capitoli e 36 articoli, la Convenzione impone diversi obblighi secondo l'approccio regolatorio basato sul rischio, il principio di trasparenza e di controllo, il principio di uguaglianza e di non discriminazione, rivolgendo una particolare attenzione alla tutela delle persone vulnerabili (persone con disabilità e minori) e alla necessità di garantire e promuovere l'alfabetizzazione digitale.

Insieme all'Unione europea, hanno sottoscritto la Convenzione i seguenti Stati membri del Consiglio d'Europa: Andorra, Georgia, Islanda, Montenegro, Norvegia, Repubblica di Moldavia, San Marino, Regno Unito; e i seguenti Stati non membri del Consiglio d'Europa: Israele e Stati Uniti d'America.

Ai fini dell'entrata in vigore la Convenzione quadro dovrà essere ratificata da almeno cinque Stati di cui almeno tre dovranno essere membri del Consiglio d'Europa.

3.2. Raccomandazione CM/Rec(2024)5 del Comitato dei ministri del Consiglio d'Europa agli Stati membri in relazione agli aspetti etici e organizzativi sull'uso dell'IA e delle tecnologie digitali da parte dei Servizi penitenziari e di libertà vigilata

Il 9 ottobre 2024 il Consiglio d'Europa ha espresso ai suoi 46 Stati membri alcune raccomandazioni volte a garantire un uso dell'intelligenza artificiale e delle tecnologie digitali, da parte dei servizi penitenziari e di libertà vigilata, rispettoso dei diritti umani e della dignità dei detenuti e delle persone in libertà vigilata.

In particolare, l'impiego dell'IA e delle tecnologie digitali deve essere rivolto alla riabilitazione dei detenuti, in ogni caso complementare e strumentale per migliorare anche la risocializzazione e ridurre la recidiva, senza mai sostituire la relazione e la decisione umana.

Nel richiamare la citata Convenzione quadro del Consiglio d'Europa sull'Intelligenza artificiale, sui Diritti umani, sulla Democrazia e sullo Stato di diritto (CETS n. 225), agli Stati membri è raccomandato di tutelare tra l'altro la riservatezza e l'integrità dei dati personali e di disporre delle risorse necessarie per controllare e monitorare assiduamente tale uso.

3.3. Iniziative e approcci regolatori nel Regno Unito: Artificial Intelligence (Regulation) Bill [HL]

Nel Regno Unito prosegue l'iter legislativo del "Artificial Intelligence (Regulation) Bill [HL]". Il testo presentato il 22 novembre 2023 e approvato il 10 maggio 2024 dalla House of Lords, attualmente si trova all'esame della House of Commons.

Ricordiamo che la suddetta regolamentazione sull'IA, applicabile in Inghilterra, Galles, Scozia e Irlanda del Nord, si articola in nove sezioni che prevedono tra l'altro, in analogia con il Regolamento europeo sull'IA, l'istituzione di un'autorità per l'IA (AI Authority) e spazi di sperimentazione (Regulatory sand-boxes) nonché la definizione legislativa del termine IA, compresa quella generativa.

B. DOTTRINA

1. Note, discussioni, riflessioni e commenti

Giancarlo Taddei Elmi, *Intelligenza artificiale e diritto: dalla "sperimentazione" alla regolamentazione". Breve storia della relazione tra Intelligenza Artificiale e Diritto. Seconda puntata: Anni Settanta-Novanta*

1. Gli anni Settanta: l'informatica informativa e decisionale

Negli anni Settanta, parallelamente agli studi teorici, si moltiplicano le applicazioni di IG dedicate al cosa può fare l'informatica (il *Quid*). I sistemi informativi diventano ormai operativi sia in ambiente di civil law sia di common law. Limitandoci all'Italia si segnala la concorrenza di due sistemi di information retrieval, lo Stairs dell'IBM e il Find della Univac. Il primo utilizzato presso la Camera dei Deputati per trattare elettronicamente la legislazione e gli atti parlamentari, il secondo scelto dal Ministero di Grazia e Giustizia per gestire molteplici archivi di giurisprudenza, legislazione e dottrina. Quest'ultimo, il celebre Italgiure, viene lanciato nel 1973 in occasione di un convegno organizzato per l'inaugurazione del Centro

elettronico di documentazione (CED) della Corte suprema di Cassazione, che per anni ne gestirà tutte le attività e le funzionalità².

Questi sistemi presentano documenti strutturati in campi e tecniche di ricerca restrittive ed espansive con operatori logici booleani – *and*, *or* e *not* –, troncamenti e mascheramenti morfologici che consentivano di ottenere risposte con alto tasso di precisione e richiamo. Il linguaggio di consultazione era peraltro molto complesso. Bisognerà attendere il passaggio dai sistemi operativi tipo DOS ai sistemi a finestre tipo windows degli anni Ottanta per rilevare una maggiore amichevolezza.

Accanto alla operatività di questi primi sistemi informativi vengono progettati alcuni embrionali e parziali sistemi decisionali, detti “esperti”, che avranno il massimo fulgore negli anni Ottanta e Novanta. Costavano di tre componenti, la rappresentazione di una base di conoscenza che descrive in modo formalizzato o le norme o i fatti, un meccanismo che permette di sviluppare ragionamenti o di tipo logico-inferenziale o analogico-semanticamente e un dialogo interattivo detto interfaccia tra utente e consulente. Il meccanismo inferenziale era costituito da insiemi di regole logiche tipo implicazioni se allora, congiunzioni *and* e disgiunzioni *or* che, combinando i vari enunciati del ragionamento, conducevano a una conclusione mentre quello analogico da strutture semantiche dirette a verificare la similarità tra fattispecie astratta e fattispecie concreta. I sistemi logico-inferenziali vengono detti anche ragionamenti a regole di produzione (*Rules based reasoning*) e quelli analogico-semanticamente ragionamenti basati sui casi (*Case based reasoning*).

Il metodo per rappresentare la conoscenza più utilizzato è inizialmente quello logico-inferenziale.

La prima proposta di un sistema basato sulle regole risale a Buchanan e Headrick³. Lo studio più rilevante dell'epoca, in ambiente di civil law, è quello di Paul Henry Steinauer⁴, che come metodo di rappresentazione della conoscenza giuridica applica la logica proposizionale riducendo le norme a enunciati e combinandoli con congiunzioni, disgiunzioni e implicazioni. La base normativa presa in considerazione è duplice: una legge fittizia sui coiffeurs⁵ e alcuni articoli della legge Comunale del Cantone di Ginevra del 1987 (LCP) e del RALCP (1958) che regolavano l'assoggettamento alla tassa professionale comunale. Appaiono già evidenti i limiti di questi sistemi. Il linguaggio giuridico è semanticamente univoco, facilmente predicabile come vero o falso e l'ampiezza normativa è minima. Gran parte del diritto invece non è costituito da norme univoche ma da proposizioni ambigue e vaghe da interpretare; inoltre la formalizzazione logica di pochi articoli, seppure univoci, richiede un eccessivo lavoro, ingiustificato rispetto ai vantaggi della automatizzazione⁶.

Una menzione particolare merita un esperimento pionieristico, della metà degli anni settanta, di consulenza fiscale (*Taxman I e II*), forse il primo sistema esperto degno di questo nome. Oggetto è la tassazione di Corporate Reorganizations, regolata nel sottocapitolo C del Capitolo I dell'*Internal Revenue Code* del 1954. *Taxman I* si proponeva di stabilire se una riorganizzazione societaria dovesse classificarsi all'interno di uno dei tre tipi di riorganizzazione esente da imposte. La conoscenza da rappresentare era la descrizione di fatti e dei concetti previsti dalle norme. Il sistema viene considerato un prototipo di sistema basato su regole di produzione, perché il funzionamento del meccanismo inferenziale ossia il modo di ragionare è totalmente deduttivo. La conoscenza all'interno delle regole viene rappresentata però in modo dichiarativo ossia attraverso reti semantiche. È il primo esempio di sistema misto che usa sia conoscenza logica a regole sia conoscenza semantica a strutture (frame o cornici)⁷. Da segnalare anche Judith che formalizza pochi articoli del Codice civile tedesco (1975)⁸.

2. CORTE SUPREMA DI CASSAZIONE 1973.

3. POPPLE 1996, p. 24.

4. STEINAUER 1975.

5. *Ivi*, p. 167 ss.

6. *Ivi*, si veda in proposito la lunga formalizzazione da p. 205 a p. 245.

7. MCARTHY 1976, pp. 305-373.

8. POPP-SCHLINK 1975, pp. 303-314.

2. Gli anni Ottanta

2.1 Operatività della informatica informativa, separazione tra IG e DI ed esplosione dell'Informatica decisionale

Gli anni Ottanta vedono alcuni importanti mutamenti tecnologici, quali l'avvento dei calcolatori individuali e dei sistemi operativi che gestiscono interfacce grafiche a finestre, lo sviluppo delle tecnologie delle reti di collegamento fisico e dei protocolli di comunicazione, che permettono il dialogo tra sistemi operativi diversi e computer diversi, e infine la produzione di dischi compatti (CD-Rom) ad alta capacità di memoria.

Studi, ricerche e sperimentazione si indirizzano prevalentemente sul *Quid*.

L'informatica documentaria consolida la sua operatività attraverso i sistemi informativi la cui consultazione diviene molto più amichevole rispetto ai sistemi gestiti dal sistema operativo DOS. Basti ricordare la pesantezza del linguaggio di interrogazione (sotto DOS) del più importante sistema informativo italiano l'Italgiure Find costruito dal CED della Corte di Cassazione di cui riporto un esempio:

Desidero trovare i documenti su locazione o affitto purché contengano anche la parola canone e siano emanate negli anni 2000 (Sistema Italgiure)

`$pt:(loca$+affitt$)*canone*an=200X ;`

pt e **an** nomi di campo

+ e ***** simboli di or e and

\$ simbolo di troncamento

X simbolo di mascheramento

; segno di fine ricerca

: segno prima di campo

= segno di cambiamento di campo

Accanto ai citati *Italgiure/Find* e *Stairs* della Camera dei Deputati si sviluppano sistemi privati, promossi soprattutto da editori quali Giuffrè, Zanichelli, De Agostini, Utet etc., che raccolgono e forniscono in prevalenza giurisprudenza e legislazione. Grande successo riscuote il sistema realizzato dall'Istituto per la documentazione giuridica del CNR (IDG ora diventato IGSG – Istituto di informatica giuridica e sistemi giudiziari) negli anni Settanta, dedicato alla dottrina pubblicata su un gran numero di periodici giuridici italiani, chiamato Banca dei dati bibliografici. Oggi viene ancora portato avanti dall'IGSG con il nome DoGi – Dottrina Giuridica.

Si fa strada la distinzione sempre più netta tra IG (*quid*) e DI (*quid iuris*) sia nel mondo di common law sia di civil law. Basti citare i volumi di Colin Tapper, *Computer Law*, dal 1978, 1982, 1983, 1989 che non si intitolano più *Computers and Law* ma *Computer Law* (il diritto dei computer) e sono dedicati esclusivamente al *quid iuris* (DI): 1. *Property*, 2. *Liability, contract, tort, crimes, privacy*, 3. *Procedure evidence, practice*⁹.

L'accento è sempre posto sul calcolatore oggetto come strumento. I sistemi informatici anche più sofisticati operano secondo programmi a priori dettagliati in base a conoscenza esplicita, che consentono sempre di risalire alle regole poste dal programmatore. I risultati sono previsti e prevedibili e non aprono questioni di difficile attribuzione di responsabilità.

L'informatica decisionale registra un momento di grande fulgore con la diffusione di numerosi progetti per la costruzione di sistemi esperti. Questi adottano due tipi di rappresentazione della conoscenza, una logica e una analogica. La prima basata sulla produzione di regole di ragionamento (*Rules based Reasoning RBR*) e la seconda basata su strutture di similarità tra casi (*Case based Reasoning CBR*). Si parla anche di sistemi procedurali o dichiarativi.

9. TAPPER 1989.

Il preludio di questo orientamento lo si può cogliere in un numero monografico della rivista *Informatica e Diritto* (oggi diventata *Rivista italiana di informatica e diritto*) che raccoglie i contributi dei più eminenti studiosi sul tema¹⁰.

2.2. *L'informatica decisionale logica. I sistemi Rules based Reasoning (RBR)*

Tra i sistemi “logici”, promossi negli anni Ottanta, segnalo il *Latent Damage System* (LDS 1980) sulla responsabilità da prodotto che non tendeva a determinare quando questa esistesse ma era disegnato per assistere gli esperti giuristi nello stabilire i casi di responsabilità da prodotto¹¹, SARA (1980), predisposto per analizzare decisioni discrezionali attraverso l'uso di norme univoche (strict) e norme che richiedono valutazione (discretionary) a cui sono applicati dei pesi basati su correlazioni tecniche¹², LEGOL (1980) che propone di usare regole per rappresentare le norme¹³, Taxadvisor (1983) destinato ad assistere gli avvocati nel fornire pareri ai clienti sulla pianificazioni fiscali e patrimoniali¹⁴, il sistema sulla legge scozzese di divorzio¹⁵ e, infine, il sistema dell'Università di Oxford del 1985 sul *British Nationality Act*¹⁶.

Tutti questi sistemi si rivolgono a settori molto limitati e a normative tendenzialmente univoche. La rappresentazione delle norme è a regole di produzione del tipo se p allora q dove p e q possono essere proposizioni costituite da elementi legati da operatori logici *and*, *or*, *not*.

Il più famoso sistema è quello dell'Università di Oxford sul *British Nationality Act*, che intende fornire risposte automatiche in relazione alla attribuzione della cittadinanza britannica. Il testo normativo è stato ridotto a enunciati logici combinati da operatori logici *and*, *nor*, *not* e *if then* utilizzando il linguaggio Prolog e le clausole *Horn*.

Tutti i sistemi a regole puri, che utilizzano solo regole inferenziali come rappresentazione della conoscenza, si basano su enunciati di significato univoco per i quali si potesse predicare facilmente la verità o la falsità. Tale assunto si rivela un limite enorme (semantico) dato che il linguaggio giuridico è notoriamente ambiguo e vago e richiede una interpretazione per giungere a dare dei significati alle norme. Tra l'altro le interpretazioni possibili sono numerose e i risultati altrettanto molteplici. Potendo dunque questi sistemi deduttivi sviluppare esclusivamente le operazioni logiche del ragionamento giuridico, a partire da enunciati già pre-interpretati, al massimo avrebbero potuto svolgere una funzione decisionale di mera consulenza, prevedendo tante soluzioni quante sono le possibili interpretazioni, ad esempio “letterale”, “fondamentale concettuale”, “fondamentale teleologica” e così via. Resterebbe, in ogni caso, a carico del giurista-giudice la parte più nobile della decisione, ossia la scelta del metodo interpretativo e la interpretazione stessa; in definitiva tutta la sussunzione della fattispecie concreta nella fattispecie astratta¹⁷. Un tale limite semantico costringe all'angolo i sistemi esperti esclusivamente logico-deduttivi che si rivelano elefanti che partoriscono topolini.

Perché un sistema esperto possa uscire dal suo ambito ristretto di esperimento di nicchia, dovrebbe gestire ambiti giuridici più ampi, la base dovrebbe essere sia normativa sia giurisprudenziale, la rappresentazione dovrebbe essere in grado di descrivere il linguaggio ambiguo e vago e, infine, il ragionamento dovrebbe procedere non solo in modo logico-deduttivo ma anche analogico-semantico¹⁸.

10. BING-HARVOLD 1977.

11. WATERMANN-PETERSON 1980, pp. 272-275.

12. BING 1980, pp. 119-136.

13. STAMPER 1980, pp. 45-71.

14. MICHAELSEN-MICHIE 1983, pp. 240-246.

15. TADDEI ELMI 2010, p. 139 ss.

16. SERGOT-SADRI-KOWALSKI 1986.

17. Vedi a suo tempo già LOMBARDI VALLAURI 1993.

18. Su questi sistemi basati sulle regole e sui loro limiti vedi POPPLE 1996, p. 24 ss.

Per questa ragione alla fine degli anni Ottanta si pensa di progettare sistemi esperti semanticamente orientati e sistemi misti non esclusivamente logico-deduttivi, dove le tecniche *Case based Reasoning* (CBR) si affiancano variamente alle tecniche *Rules based Reasoning* (RBR).

2.3. Il quid decisionale semantico

Nei sistemi analogico-semantici, la conoscenza è rappresentata non da inferenze logiche ma da cornici e reti semantiche, i casi vengono descritti con insiemi di elementi considerati significativi poi comparati e, infine, quando le somiglianze superano le differenze si stabilisce una similarità che può portare a predire soluzioni analoghe¹⁹.

Tipici esempi di sistemi a rappresentazione semantica degli anni Ottanta sono *Shister*, *Finder* e *Hypo*²⁰.

Shister, costruito per ragionare con i casi sulle leggi del Parlamento australiano, verrà combinato con un sistema esperto medico dei primi anni Settanta Mycin a regole²¹.

Finder fornisce pareri sul diritto del *trover* cioè di colui che reperisce beni smarriti (*trover of chattels*). È un'area del diritto inglese basata interamente sui precedenti dominanti o precedenti guida e un insieme di attributi significativi giuridicamente (ad esempio "il bene quando è stato trovato era fissato al terreno o a una struttura rigida?"). Per ciascuno dei casi dominanti prevede un vettore di attributi con valore; ciascun vettore di attributi-valore rappresenta i fatti rilevanti di quel caso. L'utente fornisce a *Finder* i fatti rilevanti del caso di specie rispondendo un sì o un no per ciascuno degli attributi del problema concreto. I casi dominanti sono delle fattispecie astratte e i casi specifici sono le fattispecie concrete. Il sistema assegna un peso a ciascun attributo uguale all'inverso del variare dei valori che quell'attributo assume in tutti i casi. Usa questi pesi per trovare la distanza geometrica tra fattispecie concreta e fattispecie astratta. Per costruire una argomentazione circa il risultato probabile nel caso di specie, prende a parametro il caso più vicino in assoluto e il caso più vicino con risultato opposto, cioè il primo con risultato negativo. Colloca il caso nuovo in una posizione di similarità o di diversità rispetto ai casi base e opera per analogia calcolando il grado di similarità o di differenza tra i casi dominanti e i casi nuovi. È un confronto semantico-intensionale che compara strutture semantiche definite da elementi essenziali. Fornisce un orientamento per la decisione indicando il livello di probabilità che la questione sia risolta in modo positivo²².

Hypo (*Hypothesis*) si prefigge di costruire delle ipotesi di argomentazione in relazione a controversie sui segreti commerciali. Partendo da una serie di fatti: (a) inquadra la situazione (fattispecie concreta) in una dimensione teorica (fattispecie astratta), (b) sulla base di questa analisi reperisce i precedenti rilevanti per il caso in esame da una base di conoscenza e, infine, (c) confronta il caso con altri casi della base e mette in evidenza i precedenti che giungono a conclusioni contrarie. Suggerisce inoltre argomentazioni, fatti e precedenti che possono rafforzare i casi reperiti e sottolinea gli argomenti che l'altra parte potrebbe svolgere e i modi per indebolirli. Consta di quattro componenti:

- 1) una base di precedenti di circa 30 casi che riguardano il diritto dei segreti commerciali;

19. ASHLEY-RISLAND 1988; RISSLAND-SKALAK 1989; VOSSOS-ZELEZNIKOW-DILLON-VOSSOS 1991; KOLODNER 1992; O' LEARY 1993.

20. Sui sistemi basati sui casi tipo *Finder*, *Hypo* e *Shister* vedi POPPLE 1996, p. 38 ss.

21. Il sistema Mycin è uno dei primi sistemi a regole creato allo Stanford Medical Center per fornire pareri diagnostici e trattamento su soggetti affetti da infezioni sanguigne a un medico non esperto nel campo degli antibiotici; usa un metodo di motore inferenziale (*reasoner backward-chaining*) con catena in avanti guidata dall'antecedente per la elaborazione delle regole che hanno la forma *if.then* (MYCIN - Medical Expert Systems (Sistemi esperti in sanità) | Informatica e Ingegneria Online (vitolavecchia.altervista.org) MYCIN | artificial intelligence program | Britannica). È stato usato e in combinazione con un sistema giuridico basato sui casi il *Shister* dando vita al sistema ibrido *Shister-Mycin*. Per una ampia e analitica descrizione del sistema *Shister-Mycin* vedi O' CALLAGHAN 2003, pp. 35-101.

22. Sui sistemi a regole, *case based* e ibridi vedi O' CALLAGHAN 2003, pp. 25-33 (in specie *Taxman*, *Finder*, *CABARET*, *GREBE*).

- 2) un linguaggio di rappresentazione dei precedenti costituito da una “cornice base” (titolo, data, collegio numero sentenza, rivista di pubblicazione, nome parti, oggetto, esito precedenti citati dal collegio) a cui si agganciano altre cornici più specifiche come quella delle “parti” (natura giuridica, ruolo svolto, prodotti, ditte concorrenti), quella del “prodotto” (tipo, prodotti concorrenziali, misure di sicurezza, ecc.) e così via;
- 3) una serie di descrizioni di situazioni di fatto tipiche in materia (detti predicati fattuali) a cui viene assegnato un valore positivo o negativo dopo aver esaminato la cornice del caso di specie;
- 4) una serie di rappresentazioni teoriche (dette “dimensioni”) che vengono determinate sulla base dei dati fattuali associati al caso; esse rappresentano gli aspetti giuridicamente rilevanti della fattispecie e quindi i punti di forza o debolezza delle parti.

Il sistema di fronte a un caso concreto inizialmente individua le dimensioni. Per il segreto commerciale il sistema ha previsto 17 dimensioni tra cui, a) l'impiegato è stato pagato per cambiare datore di lavoro; b) l'impiegato fornisce mezzi al nuovo datore di lavoro; c) l'esistenza di un patto di non concorrenza; d) un patto di non concorrenza sostenuto da un compenso, ecc.

L'applicazione di una dimensione è condizionata dal verificarsi di alcuni fatti (predicati): ad esempio la dimensione d) si può applicare se a) vi è un accordo espresso, b) se una parte cerca di far valere l'accordo e c) se una parte cerca di negare l'accordo.

Il sistema per ciascuna dimensione verifica il caso per vedere se soddisfa i requisiti necessari della dimensione. Successivamente recupera i precedenti che presentano le stesse dimensioni del caso in esame, stabilendo poi con un modulo di comparazione se il caso recuperato sostiene la posizione ipotetica di una parte in relazione a una particolare dimensione.

In relazione alla dimensione “compenso ricevuto per il patto di non concorrenza”, se nel caso in esame non è stato ricevuto alcun compenso per la stipula del patto, il sistema porterà a sostegno della posizione del cliente quei precedenti in cui la corte decise in favore della parte che non ricevette tale compenso.

Hypo si basa esclusivamente su precedenti, la rappresentazione è semantica (cornici) e il ragionare è analogico. Si nota anche in questo caso l'esiguità del problema e della base di conoscenza. Più aumenta l'ampiezza del settore giuridico più cresce la difficoltà di rappresentare il diritto²³.

2.4. Il Quid decisionale ibrido

Per sommare i vantaggi del metodo logico e di quello analogico, tra la fine degli anni Ottanta e l'inizio anni Novanta, vengono progettati sistemi ibridi che combinano rappresentazioni della conoscenza logico-deduttive e rappresentazioni semantiche.

Due sono i metodi per combinare RBR e CBR. Il primo, noto come “architettura lavagna” (*blackboard architecture*), prevede un numero di moduli conoscitivi interagenti reciprocamente che usano un data base condiviso (*shared*) detto lavagna (*blackboard*). Un meccanismo di controllo, pianificatore (*scheduler*) decide quale modulo cognitivo è il più adeguato per ciascuna fase del processo di ragionamento. Due sistemi tipici esempi di questa metodologia sono *Cabaret* e *Prolexs* citati più avanti. L'altro metodo di combinazione tra RBR e CBR è la IA distribuita (*distributed artificial intelligence*). Permette ai sistemi di sfruttare allo stesso tempo le proprie conoscenze di base, sia per porre domande reciproche sia per rispondere.

Il più importante sistema ibrido di tipo lavagna (*blackboard*) è *CABARET* che si occupa di una piccola area all'interno del diritto tributario, le *home office deductions*. Usa il metodo a regole e il metodo analogico come strumenti di ragionamento paralleli, ciascuno capace di operare per proprio conto.

Altri sistemi ibridi dell'epoca sono *Shister-Mycin*, *Ikbals* e *GREBE*. Il primo è un classico esempio di sistema ibrido che unisce ragionatori a regole (*Mycin*) e ragionatori sui casi (*Shister*). Si combina a *Mycin* per risolvere i concetti vaghi (*open texture*) contenuti nelle regole “*if then*”²⁴. *Ikbals*, con oggetto il diritto

23. RISSLAND-ASHLEY 1987; BENCH-CAPON 2017; TADDEI ELMI 2010, pp. 141-142; POPPLE 1996, pp. 42-43; ASHLEY 1991, pp. 753-796.

24. Per una ampia e analitica descrizione del sistema *Shister-Mycin* vedi O' CALLAGHAN 2003, pp. 35-101.

creditizio, è ibrido nel senso che con la tecnica della IA distribuita utilizza in sequenza i due metodi *RBR* e *CBR*. Alcuni ritengono in proposito che sarebbe stato più fecondo usare i due metodi in parallelo e non in modo seriale²⁵.

Il sistema *GREBE* (*Generator of Recursive Exemplar-Explanations*), che si occupa del diritto risarcitorio dei lavoratori del Texas, è ibrido perché combina sia l'architettura parallela (*shared*) lavagna (*blackboard*) sia metodi di IA distribuita. A differenza dei sistemi "lavagna" puri non prevede l'agente *scheduler*: la scelta tra le argomentazioni create dai ragionatori è fatta dopo che essi hanno costruito le loro argomentazioni; *RBR* e *CBR* sono attivati allo stesso tempo, scorrendo in modo concorrente secondo la distributed AI, fino al risultato finale che è il migliore dei due risultati prodotti, uno con *RBR* e uno con *CBR*. La base *RBR* di *GREBE* contiene 47 regole che includono leggi, common law e regole di senso comune (*common sense*). La base casistica ha 25 precedenti che includono 21 casi ipotetici. Usa anche un mixage di metodi rispetto ai casi che sono rappresentati sia con regole sia con sistema semantico (rete semantica). Questa scelta viene da alcuni criticata e considerata inappropriata²⁶.

Questi sistemi ibridi mostrano un lodevole tentativo di allargare il ventaglio dei metodi di ragionamento, però l'ambito di applicazione resta minimo a prova che il vero grande ostacolo dei sistemi esperti è la vastità del dominio da trattare²⁷.

Inoltre con i metodi analogici non si elimina il principale problema dei sistemi esperti logico-deduttivi perché tutto dipende da una determinazione degli elementi rappresentativi del caso. E determinare i molti elementi da comparare e valutare il grado di somiglianza o di differenza sono operazioni tipicamente semantiche. Anche qui entra l'interpretazione dei fatti; come nel metodo deduttivo era necessaria l'interpretazione degli enunciati normativi, così nel metodo casistico si deve dare un significato preciso ai fatti. I fatti, come le norme, non sono facilmente binarizzabili, riducibili a 0 o 1, vero falso.

Si deve però riconoscere che, mentre i sistemi simbolici basati su regole della logica si mostrano totalmente inadatti a rappresentare il ragionamento giuridico, quelli simbolici casistici basati sulla ricerca della similarità di situazioni fattuali, pur conservando alcuni limiti del simbolico-deduttivo, aprono la strada verso la tecnologia di IA c.d. connessionista o sub-simbolica. Non rappresentano in ogni caso quel salto qualitativo auspicato in relazione alla rappresentazione della conoscenza che resta sempre "esplicita". Il vero mutamento potrebbe essere offerto dal paradigma connessionista e dalla tecnologia delle reti neurali che si affacciano con prepotenza negli anni Novanta.

3. Gli anni Novanta: l'informatica reziaria e la questione soggettività dei sistemi di IA

3.1. Il quid informativo reziario

Nel corso degli anni Novanta la rivoluzione tecnologica di Internet incide profondamente sulla informatica informativa classica. I sistemi c.d. proprietari pubblici e privati vengono soppiantati dalle risorse della Rete globale. Si passa dalle banche dati reali alle banche dati virtuali, dove indice e archivio non risiedono nella stessa macchina. L'indice si trova presso il gestore del sistema e l'archivio è distribuito su altre macchine della rete. Sono dette anche motori di ricerca e sono costituite da tre programmi, uno di navigazione, uno di indicizzazione e uno di information retrieval. Il vantaggio è dato dalla grande capacità di ricerca sotto il profilo quantitativo – navigando sulla rete globale Internet –, mentre il limite è nella scarsa selettività della ricerca che si svolge su documenti eterogenei e non strutturati. Per limitare il rumore e accrescere la precisione delle risposte si deve combattere questo caos informativo con la predisposizione di portali, directories e altri strumenti che raccolgano le informazioni reperibili in ambiti più omogenei. Il paradigma reziario, dal punto di vista informativo, non è un grande passo in avanti, mentre apre nuovi scenari forse di successo nel campo del quid decisionale.

3.2. Il quid decisionale reziario o biologico. Dal "logico-analogico" al "biologico"

25. *Ibidem*.

26. Su *GREBE*, v. POPPLE 1996, p. 44 ss.

27. Sui sistemi ibridi tipo *CABARET* e altri simili vedi POPPLE 1996, p. 44 ss.

3.2.1 Le reti neurali

Con gli anni Novanta, per superare i limiti posti dalla conoscenza esplicita, ci si è orientati verso un approccio di modellizzazione della intelligenza basato su regole tratte implicitamente in modo empirico. La tecnologia più omogenea a questa metodologia, diretta a rappresentare a posteriori la conoscenza, è sembrata quella delle reti neurali che emulano il funzionamento connessionista del cervello.

La rete neurale artificiale può essere definita come "... un sistema di elaborazione costituito da una serie di elementi di elaborazione semplici e altamente interconnessi, che elaborano le informazioni mediante la loro risposta di stato dinamica agli input esterni".

Gli elementi di elaborazione semplici e altamente interconnessi sono i neuroni, definiti anche nodi o unità della rete neurale. I neuroni vengono solitamente dislocati in livelli, che possono essere di tre tipi: 1) *Livello di Ingresso (Input Layer)* per ricevere le informazioni provenienti dall'esterno al fine di imparare riconoscere e processare le stesse informazioni ricevute. 2) *Livello Nascosto con le Hidden Layer* che collegano il livello di ingresso con quello di uscita e aiutano la rete neurale a imparare le relazioni complesse analizzate dai dati. Spesso i livelli nascosti sono più di uno. 3) *Livello di Uscita (Output Layer)* che mostra il risultato di quanto il programma è riuscito a imparare.

Le reti neurali sono programmate per imparare in modo autonomo dal proprio funzionamento. Il procedimento più noto e molto utilizzato nel settore giuridico è l'algoritmo di Retro-Riproduzione (*Backpropagation*). Esso prevede di confrontare il risultato ottenuto da una rete con l'output che si vuole in realtà ottenere: usando la differenza tra i due risultati prevede di modificare i pesi delle connessioni tra i livelli della rete partendo dal livello output. Questo nuovo paradigma dell'apprendimento automatico dalla esperienza, detto *machine learning*, viene accolto con entusiasmo dal mondo degli informatico-giuridici, che vi scorgono un modo per aggirare il problema principale dei sistemi esperti, consistente nel dover rappresentare a priori formalmente la conoscenza necessaria per far funzionare il sistema stesso. Anzi l'auto-apprendere empirico attribuisce al sistema un connotato di maggiore intelligenza rispetto ai sistemi che operavano in modo logico-semantico a partire da conoscenza già precostituita²⁸. Il connubio tecnologico tra reti neurali che supportano i sistemi auto apprendenti e rete informativa globale (Web) con i *Big Data* offre la base per lo sviluppo di una nuova generazione di sistemi di IA.

I sistemi cd. empirici seguono l'evoluzione delle Reti neurali. Inizialmente sono dotate di un solo livello nascosto (apprendimento superficiale, che chiamerei *Shallow* (anni Novanta), e successivamente proseguono con una pluralità di livelli apprendimento nascosti (*Deep learning*). Il che comporterà le critiche relative alla opacità del funzionamento dei sistemi di IA con un numero elevato di strati non trasparenti (le cd. *Blackbox*).

Il diritto viene ampiamente coinvolto in queste applicazioni che utilizzano metodi di apprendimento empirico. I sistemi con rappresentazione logico-semantica a priori cedono il passo ai sistemi con auto-rappresentazione empirica a posteriori prima superficiale (*shallow*), poi profonda (*deep*)²⁹. Gli ambiti applicativi non riguardano solo la informatica decisionale-consulente ma anche quella informativa³⁰.

3.2.2. I primi esperimenti neurali shallow learning

I progetti neurali giuridici inizialmente usano un solo livello nascosto (*Shallow Learning*). Tra i primi si segnalano:

- a) *Index Theft Act* presentato nel 1994 da J. B. Hobson e D. Slee con oggetto la legge inglese sul furto³¹;

28. Sul passaggio dal paradigma logico dei sistemi esperti al paradigma empirico dei sistemi auto-apprendenti vedi KETTLEWELL 2019, pp. 8-15.

29. WINKLER 2017.

30. HUNTER 1999, pp. 129-151: studia le applicazioni delle prime reti neurali al diritto e le critica non perché il connessionismo sia inerentemente inappropriato per il diritto ma perché è stato realizzato in modo inadeguato.

31. HOBSON-SLEE 1994, p. 47.

- b) *Prolexs* realizzato presso il Computer/Law Institute dell'Università Vrije di Amsterdam dedicato al dominio delle locazioni di immobili³²;
- c) *Split up*, realizzato nel 1991 da La Trobe University di Melbourne, mira a implementare la disciplina sulla ripartizione dei beni dei coniugi dopo lo scioglimento del matrimonio come previsto dal Family Act australiano del 1975³³;
- d) *Mairilog*, sviluppato nei primi anni Novanta, utilizza le reti neurali per trarre regole logiche dalle decisioni del Consiglio di Stato in materia di Polizia municipale da usare come base di conoscenza per un sistema esperto³⁴; il sistema vive più fasi di sviluppo, una prima classica basata in modo ibrido sui ragionatori RBR e CBR e una seconda dove vengono utilizzate le reti neurali;
- e) il Progetto italo-tedesco per stabilire la responsabilità dei veicoli a motore, nato da un modello neurale di Philipps e delineato in una tesi di laurea discussa presso l'Università G. D'Annunzio di Pescara³⁵; la base di conoscenza sono 200 precedenti giurisprudenziali relativi a incidenti automobilistici tra due veicoli a un incrocio. Le decisioni codificate tramite indici sono state ridotte a un ristretto numero di variabili che dovrebbero permettere di descrivere la quasi totalità degli incidenti indicizzati.

3.3. *Il quid iuris: tutela e personalità dei sistemi di intelligenza artificiale*

Nei primi anni Novanta, quando Robotica e Intelligenza artificiale sono ancora agli albori, ci si comincia a porre la questione filosofica e giuridica a un tempo se gli artefatti informatici iper-intelligenti potrebbero un giorno superare la classica dicotomia cosa-persona così da giustificare una tutela non solo come oggetti ma anche come soggetti. L'interrogativo si iscrive in una ricerca, dedicata al "Meritevole di tutela", diretta a censire tutte le entità degne di protezione, secondo il criterio del valore (oggetti) e della soggettività (soggetti). Particolare attenzione veniva posta verso le soggettività marginali umane che non possono tutelarsi da sé come l'embrione, i minorati mentali, i malati terminali, le soggettività animali e le soggettività artificiali come i robot dotati di intelligenza³⁶.

Nel mio saggio, intitolato *I diritti dell'intelligenza artificiale tra soggettività e valore: fantadiritto o ius condendum?*³⁷, vengono definiti i criteri per attribuire agli artefatti informatici la tutela per valore e per riconoscere la tutela per soggettività. Quelli del valore sono la "complessità ed elevatezza di funzioni", la "utilità" e la "rarietà-originalità". Le tre proprietà possono presentarsi variamente combinate in modo da ottenere programmi informatici: 1) utili, semplici e comuni (non rari quantitativamente e/o non originali qualitativamente); 2) utili, elevati e comuni; 3) utili, semplici e rari; 4) utili, elevati e rari; 5) inutili, elevati e comuni; 6) inutili, elevati e rari; 7) inutili, semplici e comuni; 8) inutili, semplici e rari, ecc. È ovvio che all'interno delle antinomie utilità-inutilità, elevatezza/complessità-semplicità e rarità/originalità-diffusione esiste una gradualità che accresce il ventaglio della tipologia dei programmi.

I criteri della soggettività assoluta o ontologica sono invece la "percezione-sensazione", la "immaginazione-fantasia", la "intellegione", la "autocoscienza" e la "autodeterminazione".

La sensazione-percezione è avvertire stimoli fisici esterni, la immaginazione-fantasia la capacità di rappresentarsi anche enti sensibili, materiali anche non presenti, l'intellezione la capacità di comprendere *totum simul* il significato del discorso, la autocoscienza è il rendersi conto di ciò che accade e l'autodeterminazione è il prendere scelte in modo libero e consapevole in modo autodiretto e non eterodiretto³⁸.

32. WALKER-OSKAMP-SCHRICKX et al. 1991, pp. 35-67; OSKAMP-WALKER-SCHRICKX-VAN DEN BERG 1989 pp. 54-62; il sistema Prolexs è commentato anche in O' CALLAGHAN 2003, dove viene descritto come sistema ibrido che combina RBR e CBR.

33. ZELEZKNICOW-STRANIERI 1997; ZELEZKNICOW-STRANIERI 1995, pp. 185-194.

34. BOUCHERAU 1991, p. 288.

35. ROMEO 2012, p. 150, nota 28.

36. LOMBARDI VALLAURI 1990, pp. VIII-XCVI.

37. TADDEI ELMI 1990, pp. 685-688.

38. LOMBARDI VALLAURI 2002, p. 35 ss.

Questi requisiti sono in parte presenti nei sistemi di intelligenza artificiale dell'epoca ma a livello inconsapevole, in uno stato di sonnambulismo. Il Sistema di Intelligenza Artificiale sente ma non si accorge di sentire, riconosce significanti ma non comprende significati, non ha consapevolezza di sé e non decide in modo autonomo e cosciente. Per cui le entità artificiali anche molto intelligenti non superano la soglia della "cosalità" e gli strumenti di protezione sono da rinvenirsi nelle categorie giuridiche del brevetto, del diritto d'autore e del segreto industriale. Restano oggetti tutelabili solo per valore. Al massimo si può pensare a una soggettività attribuita (ascrittiva) dall'ordinamento come quella conferita alle associazioni e agli enti³⁹.

Nel corso degli anni Novanta, il progresso della Intelligenza Artificiale, della Robotica e della Rete sono tali che queste "cose" si diffondono sempre più cominciando a svolgere azioni non solo di supporto ma anche di sostituzione dell'uomo. Vengono chiamate agenti-software per sottolineare il carattere dinamico rispetto alle mere cose tradizionalmente statiche⁴⁰. Sul piano giuridico diviene stringente il bisogno di regolare gli effetti dei comportamenti di tali agenti informatici intelligenti e ci si chiede a chi vada attribuita la responsabilità per errori e fatti illeciti da essi prodotti. Si ripropone dunque il dilemma cosa-persona; dalla sua soluzione derivano risposte in relazione alla responsabilità specialmente civile.

I SIA cose agenti della fine anni Novanta continuano a presentare il limite semantico, nel senso che riconoscono solo significanti e sequenze di significanti e non comprendono significati. Inoltre agiscono in uno stato di totale inconsapevolezza, per cui, non possedendo i requisiti minimi della soggettività ontologica, sono da considerarsi ancora delle cose.

Per risolvere la questione responsabilità, scartate ovviamente le ipotesi di soggettività assolute, si comincia ad avanzare sempre più l'idea di conferire alle entità particolarmente intelligenti, qualora l'ordinamento lo ritenesse utile, forme di soggettività ascrittive, solitamente attribuite a enti e associazioni per ragioni pratico-funzionali. Questi status discendono esclusivamente da un atto positivo di conferimento senza alcun aggancio o riferimento ontologico-naturale; possono essere attribuiti e negati a tutto (cose e persone). Casi limite, a conferma di ciò, sono lo schiavo romano, entità certamente soggetto ontologico, ma a cui l'ordinamento non conferisce la soggettività giuridica piena, e la società per azioni, entità certamente non soggetto ontologico, a cui l'ordinamento conferisce soggettività giuridica sia pure fittizia⁴¹. Il *servus* nel diritto romano era una *res* che godeva di capacità d'agire ma non di capacità giuridica⁴².

Questa idea di artefatti informatici soggetti ascrittivi, già delineata nel 1990, viene ripresa in modo favorevole dalla dottrina internazionale; Solum nel 1992⁴³ parla chiaramente di *Legal Personhood* per la Intelligenza artificiale e Allen e Widdison la evocano per i computer capaci di stipulare contratti⁴⁴.

2. Saggi e volumi

L. BECCHETTI, *Effetti dell'intelligenza artificiale sul mercato del lavoro*, in "Diritto e Pratica del Lavoro", 2024, n. 42

L'Autore affronta il tema dell'impatto dell'intelligenza artificiale nel mondo del lavoro e il ruolo fondamentale della formazione e dell'aggiornamento delle competenze dei lavoratori nonché la necessità di una normativa che incentivi l'uso etico dell'IA e la tutela dei diritti dei lavoratori.

V. FRANCESCHELLI, *Homo creator, il diritto industriale e l'intelligenza artificiale*, in "Diritto industriale", 5, 2024

39. TADDEI ELMI 1990, pp. 688-689.

40. FINOCCHIARO 2002; SARTOR 2002, pp. 57-91.

41. TADDEI ELMI 1990, p. 688 ss.

42. FRANCHINI 2020, pp. 1-18.

43. SOLUM 1992, pp. 1231-1293.

44. Allen-Widdison 1996, p. 25 ss.

I temi trattati riguardano i rapporti tra intelligenza artificiale e diritto industriale, in particolare il tema della eventuale soggettività dei sistemi di IA in relazione alle opere.

O. POLLICINO, P. DUNN, *Disinformazione e intelligenza artificiale nell'anno delle "global elections": rischi (ed opportunità)*, in "federalismi.it", 2024, n. 24

Il contributo illustra i fenomeni della disinformazione, misinformazione e malinformazione, i pericoli per il buon funzionamento della società democratica e come tali fenomeni incidono sui processi decisionali della popolazione, non solo nell'ambito nazionale. In tale contesto è analizzato, anche con un'analisi comparativa tra Stati Uniti d'America e Unione europea, l'impatto dell'IA e la pluralità dei possibili usi, tra i quali quello della produzione di materiali e contenuti di natura inerentemente disinformativa capaci di influenzare l'opinione pubblica.

G. VACIAGO, *Intelligenza artificiale generativa e professione forense*, Giuffrè Francis Lefebvre, 2024

La pubblicazione è il risultato di una sperimentazione condotta dal Tavolo Istituzionale "Intelligenza Artificiale e Giustizia" dell'Ordine degli Avvocati di Milano a proposito dell'impatto delle tecnologie di seconda generazione, in particolare dell'IA sull'avvocatura e la professione forense.

G. CASSANO, E.M. TRIPODI, *Il Regolamento Europeo sull'Intelligenza Artificiale, Commento al Reg. UE n. 1689/2024*, Maggioli, 2024

Il volume tratta nella prima parte alcune questioni in relazione a IA e: difesa dei diritti e il ruolo dell'avvocato nella applicazione dei sistemi di intelligenza artificiale (Guido Alpa); profili comparati dell'IA (Roberta Raimondo); diritti costituzionali e discriminazione (Massimiliano Marotta); diritto amministrativo (Antonino Mazza Labocchetta); diritto dei contratti (Matteo Tofanelli); etica (Alfonso Contaldo); sviluppo delle competenze (Fabrizio Paonessa); proprietà intellettuale (Massimo Sterpi e Francesca Di Lazzaro); trasferimento scientifico e tecnologico (Fabrizio Paonessa); sicurezza dei prodotti (Giovanna Capilli); tutela dei dati (Saverio Cavalcanti) e GDPR (Enzo Maria Tripodi); decisioni automatizzate e il rischio di black box society (Bartolo Dattola); cybersicurezza (Francesco Amendola e Paolo Sferlazza); digital-robawars (Stefano Aterno e Paola Patriarca); impresa (Antonio Maria Russo).

La seconda parte del volume è interamente dedicata a commentare il Regolamento sull'IA: genesi (Livia Marafioti); obiettivi (Giuseppe Maria Marsico); caratteri essenziali e ambito di applicazione (Livia Marafioti); approccio basato sul rischio (Giuseppe Maria Marsico); sistemi di IA (Filippo Loré); applicazioni e pratiche proibite di IA (Chiara Pappalardo); sistemi di IA ad alto rischio (Andrea Del Forno); modalità di realizzazione dei sistemi e governance sui dati, resilienza dei sistemi e controllo umano (Francesco D'Amora e Ilaria Uletto); obblighi dei fornitori: la trasparenza (Giuseppina Napoli e Francesco Serino); compliance e distribuzione commerciale dei sistemi di IA ad alto rischio (Mario Cigno e Amalia Serena Scimè); obblighi a carico degli utenti (Francesco D'Amora e Ilaria Uletto); rapporti con umani (Ludovico Anselmi); IA generativa per finalità generali e ChatGPT (Micaela Unfer); organismi notificati e valutazioni di conformità (Giulia Escurole e Federico Di Croce); codici di condotta (Nicola Sepe e Bruno Urbani); governance (Carlo Calenda); autorità nazionali competenti (Elio Guarnaccia e Giorgio Bonaventura); compiti della Commissione per la tenuta della banca dati delle IA ad alto rischio (Simone Bonavita e Marco Alagna); altri comitati nazionali e internazionali (Andrea Mezzetti e Caterina Chiari); monitoraggio dopo l'immissione sul mercato (Giovanni Adamo e Norma de Gregorio); segnalazione degli incidenti e dei malfunzionamenti (Giovanni Adamo e Norma de Gregorio); vigilanza e sistemi di controllo, sistemi che presentano rischi e rischi a livello nazionale (Gianvito Boccone); sanzioni e procedure sanzionatorie (Flaviano Peluso e Chiara Matteoni); riservatezza e segretezza (Flaviano Peluso e Giorgia Mari); misure di sostegno (Fabrizio Paonessa); modifiche alla disciplina europea e regole già esistenti (Saverio Cavalcanti e Gilberto Nava).

Infine, il volume si sofferma sul disegno di legge italiano in materia di intelligenza artificiale (Giuseppe Cassano).

C. EVENTI, SEMINARI, CONVEGNI, NOTIZIE

- Intelligenza artificiale tra valutazione del rischio e certificazione accreditata, 16 ottobre 2024, Aula Magna del Palazzo del Rettorato Sapienza Università di Roma

In occasione del Convegno dell'Osservatorio Accredia è stato richiamato lo studio "Norme tecniche e valutazione della conformità accreditata per lo sviluppo dei sistemi di Intelligenza Artificiale", realizzato in collaborazione con il Laboratorio Nazionale di Artificial Intelligence and Intelligent Systems (AIIS) del Consorzio Interuniversitario Nazionale per l'Informatica (CINI).

Al quadro di regole contenute nel Regolamento (UE) 1689/2024 si affiancano e assumono un ruolo decisivo: la normativa tecnica, la valutazione della conformità e l'accreditamento. Le norme tecniche sono necessarie per garantire la qualità dei dati, la robustezza dei sistemi di IA e per assicurare gli standard di sicurezza. Il Regolamento sull'IA ha definito la catena dei controlli e ha caratterizzato i sistemi di IA sulla base del rischio. Per applicare e rendere operativa la regolamentazione sono necessari, tra l'altro, protocolli precisi e modalità di documentazione tecnica, adeguatezza delle risorse computazionali, consapevolezza dei processi, formazione. Nel contesto internazionale è necessario realizzare un maggiore allineamento e livello di standardizzazione, il riferimento agli standard ISO è fondamentale.

- Intelligenza Artificiale Amministrativa (IIA). Principi e regole per l'esercizio delle funzioni pubbliche, 4/5 luglio 2024, Palazzo Wedekind, Piazza Colonna, Roma

Nel corso del convegno sono stati esaminati, anche in prospettiva europea, i principi e criteri giuridici inerenti all'applicazione dell'IA alla funzione pubblica. Il convegno è stato organizzato nell'ambito del PRIN 2022 "Artificial Administrative Intelligence for territorial equality. Operative research over the public interest and the protection of persons in the face of the evolutions of digital era". Gli atti saranno pubblicati su uno speciale numero monografico della rivista scientifica "Amministrativ@mente", integrato anche con un'apposita call for papers.

- Intelligenza artificiale e professione forense. Le novità introdotte dall'AI ACT dell'UE, 20 giugno 2024, UnitelmaSapienza, Sala Conferenze, Roma

Il primo panel ha illustrato "Il nuovo Regolamento UE sull'Intelligenza artificiale" con gli interventi di Rino Falcone, Filippo Donati, Gianluca Contaldi, Marta Cimitile. Il secondo panel "L'intelligenza artificiale nella giurisdizione" è stato introdotto e moderato da Anton Giulio Lana. Sono intervenuti Andrea Di Porto, Fabrizio Criscuolo, Vincenzo Zeno-Zencovich, Alberto Maria Gambino.

- Intelligenza Artificiale e Stato di diritto: sfide e opportunità per le democrazie nell'era digitale, 3 maggio 2024, Camera dei deputati, Sala del Cenacolo, Roma

Organizzato dalla Fondazione Marco Pannella ETS, il convegno, suddiviso in quattro sessioni tematiche, ha trattato alcune delle questioni principali dell'IA: (1) IA e diritti umani: tra Innovazione e Tradizione - Come può l'IA essere armonizzata con i principi universali dei diritti umani, bilanciando progresso tecnologico e valori tradizionali? (2) IA e democrazia digitale: I nuovi algoritmi della partecipazione - In che modo l'IA sta ridefinendo le modalità di partecipazione democratica e quali sono le sue implicazioni per la rappresentanza e l'inclusione? (3) IA e informazione: decodificare la verità in rete - Quali sono le sfide e le opportunità poste dall'IA nella gestione e nella validazione delle informazioni nell'era della post-verità? (4) IA e policy: progettare un futuro etico nell'era digitale - Come possono i decisori politici e gli sviluppatori di IA collaborare per garantire che l'evoluzione dell'IA sia guidata da principi etici e responsabili?

Sul sito web della [Fondazione Marco Pannella](#) è possibile leggere e scaricare gli atti del convegno e rivedere la registrazione video integrale dell'evento.

Riferimenti bibliografici

- T. ALLEN, R. WIDDISON (1996), *Can Computers Make Contracts?*, in "Harvard Journal of Law and Technology", vol. 9, 1996, n. 1

- K.D. ASHLEY (1991), *Reasoning with cases and hypotheticals in HYPO*, in “International Journal of Man-Machine Studies”, vol. 34, 1991, n. 6
- K.D. ASHLEY, E.L. RISSLAND (1988), *A case-based approach to modeling legal expertise*, IEEE Expert, vol. 3, 1988, n. 3
- T.J.M. BENCH-CAPON (2017), *HYPO’S legacy: introduction to the virtual special issue*, in “Artificial Intelligence and Law”, vol. 25, 2017
- J. BING (1980), *Legal norms, discretionary rules and computer programs*, in B. Niblett (ed.), “Computer Science and Law”, Cambridge University Press, 1980
- J. BING, T. HARVOLD (1977), *Legal Decisions and Information Systems*, Universitetsforlaget, 1977
- L. BOUCHERAU (1991), *Extracting Legal Knowledge by Means of a Multilayer Neural Network Application to Municipal Jurisprudence*, in “Third International Conference on Artificial Intelligence and Law”, 1991
- CORTE SUPREMA DI CASSAZIONE (a cura di) (1973), *Atti del Convegno sulla Diffusione delle informazioni giuridiche con l’ausilio degli elaboratori elettronici*, Edizioni INFORAV, Arte della stampa, 1973
- P. FALLETTA, A. MARSANO (2024), *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull’intelligenza artificiale e GDPR*, in “Rivista italiana di informatica e diritto”, 2024, n. 1
- G. FINOCCHIARO (2002), *La conclusione del contratto telematico mediante i software agents: un falso problema giuridico?*, in “Contratto e Impresa”, 2002, n. 2
- L. FRANCHINI (2020), *Disciplina romana della schiavitù ed intelligenza artificiale odierna. Spunti di comparazione*, in “Diritto Mercato Tecnologia”, 8 luglio 2020
- J. HOBSON, D. SLEE (1994), *Indexing the Tefht Act 1968 for case based reasoning (CBR) and Artificial Neural Networks (ANNs)*, in “Fourth International Conference on Artificial Intelligence and Law, Computers and Artificial Intelligence”, 1994
- D. HUNTER (1999), *Out of their minds: legal theory in neural networks*, in “Artificial Intelligence and Law”, vol. 7, 1999
- W.J. KETTLEWELL (2019), *L’intelligence artificielle en droit: Mithes, Réalités et Consequences*, ULB, Working Paper 2019-1
- J.L. KOLODNER (1992), *An Introduction to Case-Based Reasoning*, in “Artificial Intelligence Review”, vol. 6, 1992
- L. LOMBARDI VALLAURI (2002), *Riduzionismo e Oltre*, Cedam, 2002
- L. LOMBARDI VALLAURI (1993), *Verso un sistema esperto giuridico integrale*, in C. Ciampi, F. Socci Natali, G. Taddei Elmi (a cura di), *Atti del Convegno “Verso un sistema esperto giuridico integrale”*, Cedam, 1993
- L. LOMBARDI VALLAURI (1990), *Abitare pleromaticamente la terra*, in Id. (a cura di), “Il meritevole di tutela”, Giuffrè, 1990
- T. MCARTHY (1976), *Reflections on TAXMAN: An Experiment in Artificial Intelligence and Legal Reasoning* (original version), in “Harvard Law Review”, 1976, n. 5
- R. MICHAELSEN, D. MICHIE (1983), *Expert Systems in business*, in “Datamation”, vol. 29, 1983
- T.A. O’ CALLAGHAN (2003), *A Hybrid Legal Expert System*, The Australian National University, 2003
- D.E. O’ LEARY (1993), *Verification and Validation of Case-Based Systems*, in “Expert Systems with Applications”, vol. 6, 1993, n. 1

- A. OSKAMP, R.F. WALKER, J.A. SCHRICKX, P.H. VAN DEN BERG (1989), *Prolexs divide and rule. A legal application*, in "ICAAIL '89: Proceedings 2nd International conference on Intelligence artificial and law", ACM, 1989
- W.G. POPP, B. SCHLINK (1975), *A computer program to advise lawyers in reasoning case*, in "Jurimetrics", vol. 15, 1975, n. 4
- J. POPPLE (1996), *A Pragmatic Legal Expert System*, Bookfield USA, 1996
- E.L. RISSLAND, K.D. ASHLEY (1987), *A case-based system for trade secrets law*, in "ICAAIL '87: Proceedings of the 1st International Conference on Artificial intelligence and law", ACM, 1987
- E.L. RISSLAND, D.B. SKALAK (1989), *Case-Based Reasoning in a Rule-Governed Domain*, in "Proceedings of the Fifth IEEE Conference on Artificial Intelligence Applications", Institute of Electrical and Electronics Engineers, 1989
- F. ROMEO (2012), *Lezioni di informatica giuridica*, Giappichelli, 2012
- G. SARTOR (2002), *Gli agenti software nuovi soggetti del ciberdiritto*, in "Contratto e Impresa", 2002, n. 2
- M.J. SERGOT, S. SADRI, A. KOWALSKI et al. (1986), *The British Nationality Act as a Logic Program*, Communications of the ACM, vol. 29, 1986, n. 5
- L.B. SOLUM (1992), *Legal Personhood for Artificial Intelligences*, in "North Carolina Law Review", vol. 70, 1992
- R. STAMPER (1980), *LEGOL Modelling legal rules by computer*, in B. Niblett (ed.), "Computer Science and Law", Cambridge University Press, 1980
- P.H. STEINAUER (1975), *L'Informatique et l'application du droit. Le Role du juriste dans l'élaboratin d'un programme d'application par ordinateur*, Editions Universitaires, 1975
- G. TADDEI ELMi (2010), *Corso di informatica giuridica*, Simone, 2010
- G. TADDEI ELMi (1990), *I diritti dell'intelligenza artificiale tra soggettività e valore: fantadiritto o ius condendum?*, in L. Lombardi Vallauri (a cura di), "Il meritevole di tutela", Giuffrè, 1990
- C. TAPPER (1989), *Computer Law*, fourth edition, Longman, 1989
- G. VOSSOS, J. ZELEZNIKOW, T. DILLON, V. VOSSOS (1991), *An example of Integrating Legal Case Based Reasoning with Object-Oriented Rule-Based Systems: IKBALS II*, in "Proceedings of the Third International Conference on Artificial Intelligence and Law", Association for Computing Machinery, 1991
- R.F. WALKER, A. OSKAMP, J.A. SCHRICKX et al. (1991), *Prolexs: Creating Law and Order in a Heterogeneous Domain*, in "International Journal Man-Machines Studies", vol. 35, 1991, n. 1
- D. WATERMANN, M. PETERSON (1980), *Rules based models legal expertise*, in "Proceedings of the AAAI Conference on Artificial Intelligence", AAAI Press, 1980
- D.A. WINKLER (2017), *Performance of Deep and Shallow Neural Networks, the Universal Approximation Theorem, Activity Cliffs, and QSAR*, in "Molecular Informatics", vol. 36, 2017, n. 1-2
- J. ZELEZNIKOW, A. STRANIERI (1997), *Modelling Discretion in Split Up System*, in "PACIS 1997 Proceedings", 1997
- J. ZELEZNIKOW, A. STRANIERI (1995), *The split-up system: integrating neural network and rule based-reasoning in the legal domain*, in "ICAAIL '95: Proceedings of the 5th international conference on Artificial intelligence and law", ACM, 1995



RIVISTA ITALIANA DI
INFORMATICA E DIRITTO

PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0202 • articolo non sottoposto a peer review • pubblicato in anteprima il 23 dic. 2024
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale 

MARCO FABRI

Recensione a: Paola Lucarelli (a cura di), *Giustizia sostenibile. Sfide organizzative e tecnologiche per una nuova professionalità*, Firenze, University Press, 2023, pp. 272

L'Autore è dirigente di ricerca presso l'Istituto di Informatica Giuridica e Sistemi Giudiziari del CNR sede di Bologna

Il volume è un'opera collettanea che riassume alcuni dei risultati ottenuti dal progetto "Giustizia Agile" che ha visto la partecipazione di diverse università toscane, laziali e umbre. Il progetto "Giustizia Agile" è uno dei sei progetti finanziati dal Ministero della Giustizia, con oltre 51 milioni di euro su tutto il territorio nazionale, a vari raggruppamenti universitari. I fondi provenivano dal finanziamento europeo PON governance 2014-2020. L'obiettivo ambizioso, e irrealizzabile nei tempi ristrettissimi previsti dal progetto, chiedeva alle varie università di proporre "Azioni di miglioramento dell'efficienza e delle prestazioni degli uffici giudiziari attraverso l'innovazione tecnologica, il supporto organizzativo alla informatizzazione e telematizzazione degli uffici giudiziari, disseminazione di specifiche innovazioni e supporto all'attivazione di interventi di change management". Più in dettaglio, i risultati attesi erano: «la definizione di moduli operativi da sperimentare presso gli uffici giudiziari al fine di contribuire al raggiungimento dei seguenti risultati: aumentare la produttività degli uffici, riducendo i tempi di lavorazione delle pratiche; migliorare la qualità del lavoro di giudici e cancellieri; supportare il processo di digitalizzazione ed innovazione tecnologica per giudici e cancellerie; aumentare l'utilizzo delle tecnologie da parte di tutti gli stakeholder ed in particolare dei software utilizzati dai giudici, dalle cancellerie e dagli "assistenti dei giudici" ossia dai componenti dell'Ufficio per il Processo; ridurre le distanze tra i cittadini e il sistema giustizia; ridurre i tempi di attivazione ed erogazione dei servizi di informazione per l'inoltro delle istanze/ricorsi; rafforzare l'immagine del "Sistema Giustizia per il Territorio"; individuare metodi uniformi per ridurre l'arretrato civile; rafforzare le sinergie tra sistema della giustizia e sistema della formazione e della ricerca universitaria; adeguare l'offerta formativa alle esigenze del sistema giudiziario. Non c'è che dire, un "vaste programme". I [risultati di questo investimento](#)

[relativi a tutti i progetti](#) sono disponibili sulle pagine web del Ministero della Giustizia.

Questo libro propone una prefazione e dodici contributi suddivisi in tre parti: 1) i problemi, che contiene sei contributi, 2) i modelli per l'efficienza, in cui sono stati inseriti quattro contributi 3) l'utilità della ricerca empirica, con due contributi.

Il primo saggio, scritto da Paola Lucarelli, affronta con un approccio originale la "sostenibilità" del sistema giustizia, che lo è «se si presentano le condizioni per rispondere alla domanda di tutela nel rispetto dei principi costituzionali e della legge ordinaria, primo fra tutti il principio della ragionevole durata del processo» (p. 19). L'idea alla base è quella di un maggior utilizzo del dialogo e della collaborazione nella gestione delle liti, affinché «coloro che si saranno appropriati della cultura dell'uso parsimonioso e oculato del servizio giustizia agiranno più consapevolmente risparmiando le altre risorse del pianeta» (p. 22). Non sono totalmente convinto che questa tesi così suggestiva si possa effettivamente applicare al giudiziario, il dialogo e la collaborazione, ed aggiungerei la ragione, sono certamente da utilizzare per cercare di risolvere e non esasperare un conflitto, con chiari benefici sia per chi quel conflitto è chiamato a dirimerlo, sia per chi invece ne è parte. Assolutamente condivisibile il passaggio in cui si scrive che occorre cogliere il «passo decisivo per il superamento dell'idea che i problemi della giustizia possono essere affrontati e risolti solo attraverso la riforma delle regole processuali» (p. 24). Le regole processuali sono importanti ma l'organizzazione dell'ufficio con tutte le sue componenti: umana, tecnologica, strutturale etc. è il cuore del buon funzionamento dell'amministrazione giudiziaria.

Il secondo contributo di Vincenzo Cavaliere ha un taglio aziendalistico e si sofferma su alcuni aspetti dell'organizzazione che stanno diventando sempre più importanti anche per l'amministrazione giudiziaria e che vennero introdotti, nei primi anni novanta del secolo scorso, dagli studi del Prof.

Giuseppe Di Federico del Centro Studi sull'Ordinamento Giudiziario dell'Università di Bologna e poi dai suoi allievi dell'Istituto di Ricerca sui Sistemi Giudiziari del Consiglio Nazionale delle Ricerche. I concetti di efficacia, efficienza, case management, court management, considerati per anni alla stregua della blasfemia da giuristi e magistrati, fanno ora parte dell'agenda politica e del dibattito sull'amministrazione della giustizia. In questi anni vi sono stati certamente alcuni risultati positivi, ma molto resta ancora da fare. Interessante il passaggio sul «grado di equità e giustizia organizzativa percepito dall'individuo [che ne] determina quindi la sua decisione a continuare o desistere dall'azione e in ultima analisi l'efficienza e l'efficacia organizzativa» che calza a pennello sulle opportunità, ma anche sui rischi, dell'istituzione dell'ufficio per il processo molto volte richiamata nel volume.

Annalisa Tonarelli entra negli uffici per il processo di alcuni tribunali e di una corte di appello e ne analizza le dinamiche sociali delle persone che lo compongono, magistrati, personale di cancelleria e addetti reclutati ad hoc. In particolare, l'autrice si sofferma sulle necessità formative degli addetti, sulle dotazioni informatiche e sugli spazi, sulle definizioni di compiti e funzioni e su come questi aspetti siano stati affrontati dal ministero. Emergono ampi margini di miglioramento; a fronte del «clima positivo percepito [non vi è stato] un altrettanto miglioramento della qualità del lavoro» (p. 79). L'analisi sul campo, ma anche i monitoraggi del ministero, hanno mostrato realtà molto diverse circa l'impiego degli addetti all'ufficio per il processo, con situazioni in cui sono stati destinati alla cancelleria, alle sezioni giurisdizionali, oppure ad un singolo giudice. I vari impieghi hanno di fatto risposto alle reali esigenze, o percepite come tali, di ogni singolo ufficio e sono anche dipese dalle capacità gestionali del presidente del tribunale e del dirigente amministrativo. Più che un «ufficio per il processo», come è stato chiamato, credo si tratti di fatto di un «ufficio del giudice, della sezione, o della cancelleria» a seconda dei casi.

Il contributo successivo di Ilaria Pagni riguarda un tema strettamente giuridico relativo alla riforma del codice di procedura civile ed il suo impatto alla prova dei fatti. Ormai credo si sia perso il conto sia delle «riforme epocali» sia di quelle «puntuali», tutte però di scarso successo. Forse sarebbe ora di inserire nelle commissioni ministeriali che

si occupano di questioni procedurali anche altre professionalità, non solo quindi giuristi «puri», per provare ad avere risultati diversi. In fondo, come viene ricordato anche in altre parti del volume, le procedure sono importantissime in qualsiasi organizzazione, ma non hanno solo una componente formale ma anche informale, le pratiche, e sono queste ultime che spesso ne decretano il buono o il cattivo funzionamento.

Margherita Cassano e Carlotta Conti approfondiscono gli obiettivi della riforma penale. Le autrici indicano un aspetto certamente positivo il tentativo di rafforzare le garanzie e velocizzare il processo per renderlo più vicino ai tempi degli altri paesi europei, ma non sottacciano che ci sono altre letture della riforma che la qualificherebbero come «uno slittamento verso una soave inquisizione» (p. 102). Segue un'interessante analisi delle varie modifiche apportate dalla riforma che credo dovranno essere valutate in concreto, empiricamente, negli uffici giudiziari per verificarne il funzionamento.

L'ultimo contributo della prima parte è di Emilio Santoro e riguarda un approfondimento della sezione specializzata immigrazione del tribunale di Firenze, sezione che in alcuni uffici soprattutto del Nord Italia ha numeri imponenti, e pertanto contribuisce in maniera molto significativa al calcolo degli obiettivi PNRR da raggiungere. Il progetto «Giustizia Agile», più che sui numeri, si è concentrato sugli aspetti sostanziali di tutela dei diritti fondamentali provenienti dalle richieste di protezione internazionale di soggetti vittime di sfruttamento lavorativo. Credo che la sezione specializzata immigrazione è forse quella che si presta maggiormente, se ben organizzata, al contributo degli addetti all'ufficio per il processo per le caratteristiche della materia trattata. Questo saggio, si sofferma sull'organizzazione del lavoro degli addetti con indicazioni che possono essere utili anche per altri uffici. Interessante è l'idea di una «libreria della sezione» per la documentazione raccolta che a mio parere potrebbe essere estesa a livello nazionale.

La seconda parte del volume è dedicata ai «modelli per l'efficienza». È forse opportuno qui ricordare la differenza fra efficacia ed efficienza che talvolta sono confusi. In estrema sintesi, l'efficacia misura il raggiungimento del risultato che ci siamo prefissati, l'efficienza il rapporto fra risultati

raggiunti e risorse impiegate. Quindi il raggiungimento degli obiettivi di disposition time fissati dal PNRR sono un misura di efficacia; il numero di magistrati e addetti all'ufficio per il processo con cui il tribunale cerca di raggiungere quel risultato ne misura, in parte, l'efficienza.

Il primo contributo di Silvia Bacci e Valeria Tocchi si occupa di statistica giudiziaria. In questi ultimi anni sono stati fatti passi in avanti notevoli sulla disponibilità e quindi sull'analisi dei dati provenienti soprattutto dai sistemi informativi del civile. Quello che ancora manca è fondare sempre di più i processi decisionali proprio sui dati, sulle evidenze empiriche, e non su altre "variabili intervenienti" che spesso hanno ben poco a che fare con il miglioramento del funzionamento dell'amministrazione giudiziaria. Il saggio presenta una serie di interessanti indicatori statistici già utilizzati, ma anche non ancora utilizzati, dagli uffici giudiziari. La statistica giudiziaria è peculiare perché richiede non solo competenze statistiche, ma anche di funzionamento degli uffici, ed è forse per questo che nel contributo vi sono un paio di sbavature. Comunque, gli indicatori sono ben illustrati anche con esempi molto utili per chi si confronta per la prima volta con questi temi. La conclusione con cui si auspica una generale diffusione della "cultura statistica" è ovviamente condivisibile e mi pare che sia ormai ben radicata nei magistrati, considerando anche le iniziative intraprese dalla Scuola superiore della magistratura. Resta il fatto che alcune professionalità ormai fondamentali per il buon funzionamento della giustizia, tanto importanti quanto quelle dei magistrati, dovrebbero essere meglio retribuite e dovrebbero prevedere dei corretti percorsi di carriera, altrimenti risultano gioco forza poco appetibili.

Il secondo contributo di questa parte del volume è di Paola Lucarelli che torna sulla necessità di diffondere una "giustizia consensuale" a beneficio anche della sostenibilità. Il capitolo si apre con una frase fondamentale che è un po' il leitmotiv del volume: «Il funzionamento della macchina processuale è senza dubbio di importanza estrema, ma non è sufficiente» (p. 169). La costruzione della fiducia nella giustizia, la sua legittimazione passa da un «senso di partecipazione al suo funzionamento nella società e negli stessi beneficiari della giustizia» (p. 170). La risoluzione dei conflitti può trovare nella mediazione nella risoluzione

consensuale una complementarità alla tradizionale sentenza del giudice. Insomma, da un "gioco a somma zero" ad un "gioco a somma positiva" in cui non ci sia un unico "vincitore". Forse, come già le esperienze si questi anni insegnano, non tutti i procedimenti sono adatti ad essere mediati, ma il punto fondamentale sottolineato dall'autrice non è tanto negli aspetti tecnico-giuridici, seppure importanti ma, soprattutto, è il necessario cambio di mentalità, di prospettiva che dovrebbe riguardare tutti, proprio tutti, gli attori del procedimento.

Segue un contributo di Paolo Nesi sull'utilizzo di un applicativo per la valutazione della propensione alla mediazione. Il contributo è interessante, necessariamente tecnico, in un ambito disciplinare che non mi appartiene. Resta la curiosità del lettore di sapere se l'applicativo è stato, ed eventualmente lo è ancora, utilizzato dagli uffici giudiziari e quali potrebbero essere le prospettive di ulteriore sviluppo.

Il quarto saggio che chiude la seconda parte del libro è di Simone Marinai e si occupa delle procedure informatiche per la tutela della trasparenza e della riservatezza dei dati. Il contributo illustra in modo molto efficace la differenza fra "anonimizzazione", "de-identificazione" e "pseudo-anonimizzazione", con utili esempi. Nell'ambito del progetto è stato sviluppato un prototipo di anonimizzazione sulla base di 705 sentenze del tribunale di Prato che, lo stesso autore, dichiara essere "limitato sotto vari aspetti" ma soddisfacente. Sarebbe interessante vederne eventuali sviluppi anche alla luce degli investimenti che il ministero sta facendo proprio sull'anonimizzazione delle sentenze,

La terza parte del volume è dedicata all'utilità della ricerca empirica, che avrebbe dovuto essere il focus principale di tutti i progetti finanziati dal PON governance.

Il primo dei due contributi che compongono questa sezione del volume è di Edoardo Borselli e Leonardo Dani ed illustra il modello "Athena". Si tratta di uno strumento di ausilio per il giudice per gestire meglio le controversie e programmare il carico di lavoro. Lo strumento è destinato ad essere utilizzato in primis dagli addetti all'ufficio per il processo ed è costituito da tre parti. La costruzione di una linea temporale del processo, forse sarebbe stato più corretto parlare di procedimento; la cartella organizzativa condivisa con il giudice al

quale «viene mano a mano apparecchiato il tavolo di lavoro con tutto quanto possa tornargli utile in ogni specifico momento» (p. 233); e la scheda del fascicolo. Quest'ultima si compone di una parte in cui sono indicate le peculiarità del fascicolo ed una seconda parte in cui si cerca di dare un "peso numerico al fascicolo" sulla base di predeterminati criteri di complessità. Lo strumento sembrerebbe utile soprattutto per la formazione degli addetti all'ufficio per il processo, anche se appare forse un po' troppo dettagliato. Quello che non è chiaro è se sia stato, o lo sia tuttora, utilizzato negli uffici giudiziari e quale risultati ne siano derivati. La valutazione empirica è fondamentale per comprendere la reale utilità di ogni strumento o prassi applicativa ed eventualmente apportare i necessari correttivi.

L'ultimo contributo di Monica Testi si occupa della valutazione della mediabilità delle liti attraverso un modello operativo. Sono descritti i passaggi che hanno portato ad estrarre i procedimenti considerando alcune variabili attraverso l'utilizzo del "pacchetto ispettori" del ministero. Quindi ne è seguita l'analisi per la valutazione della mediabilità sulla base delle circostanze previste dalla legge (e.g. natura della causa, comportamento delle parti, stato dell'istruzione del fascicolo, e ogni altra

circostanza). Tale analisi troverebbe la sua massima utilità se inserita nell'ambito della "console del magistrato", l'interfaccia utente dell'applicativo che i giudici usano nell'ambito del processo civile telematico. Il contributo è interessante, ma come è successo anche per alcuni altri saggi contenuti in questo volume, manca la descrizione dettagliata di quanto è stato fatto sul campo negli uffici. Resta così la curiosità se questa modalità di valutare la mediabilità dei procedimenti sia stata effettivamente utilizzata, da quanti giudici, con quale apprezzamento, con quali criticità, e soprattutto con quali risultati. Aspetti fondamentali che sarebbero utili anche per replicare l'esperienza in altri uffici giudiziari.

Il volume è interessante e tratta una pluralità di temi che sono certamente importanti per il miglioramento del funzionamento dell'amministrazione della giustizia. Purtroppo, i vari contributi sono un po' slegati fra loro, manca un filo conduttore, probabilmente anche perché sono figli di un progetto finanziato dal Ministero della Giustizia che poi non ha svolto l'indispensabile ruolo di stimolo, di coordinamento, di valutazione e di eventuale valorizzazione dei vari progetti. 51 milioni di euro non sono pochi, speriamo non siano stati sprecati.

Autori del 2024

BENEDETTA AGOSTINELLI Università degli Studi Roma Tre
ENRICO ALBANESI Università di Genova
FRANCESCA BAILO Università di Genova
TERESA BALDUZZI Università degli Studi Roma Tre
GIOVANNI BAROZZI REGGIANI Università di Sassari
FAVORITA BARRA LUISS Guido Carli
DANIELLE BORGES European University Institute – Florence
ELDA BROGI European University Institute – Florence
VILARD BYTYQI Kosovo Academy for Public Safety
DORINDA CACCIOPPO Università degli Studi Roma Tre
SIMONE CAFIERO Università degli Studi di Napoli Federico II
VINCENZO CALDERONIO Università di Pisa
FEDERICA CAMILLERI Università di Pisa
TONINO CANTELM Università Gregoriana – Roma
ENRICO CARLONI Università di Perugia
FEDERICA CASAROSA Scuola Superiore Sant'Anna di Pisa
PIER GIORGIO CHIARA Università di Bologna
LILIANA CILIBERTI Università degli Studi di Milano
RICCARDO MICHELE COLANGELO Universitas Mercatorum – Roma
CARLO COLAPIETRO Università degli Studi Roma Tre
PAOLO COMOGLIO Università di Genova
JACOPO DELLA TORRE Università di Genova
MARCO FABRI – Istituto di Informatica Giuridica e Sistemi Giudiziari – CNR
MATTEO FALCONE Università di Perugia
PIETRO FALLETTA Università dell'Insubria
GIANLUCA FASANO Istituto di Scienze e Tecnologie della Cognizione – CNR
GAIA FIORINELLI Scuola Superiore Sant'Anna di Pisa
ILDE FORGIONE Ministero dell'Economia e delle Finanze
MICHELE FRANCAVIGLIA Università di Genova
MATTEO GIANNELLI Università degli Studi di Firenze
OTTAVIO GRANDINETTI Università degli Studi di Napoli Suor Orsola Benincasa
STEFANO BRUNO GRENCI Formez PA
ANTONIO IANNUZZI Università degli Studi Roma Tre
TANJA KERSEVAN European University Institute – Florence
FERNANDO H. LLANO ALONSO University of Seville
LUISA LODEVOLE Università degli Studi di Roma Tor Vergata
ERIK LONGO Università degli Studi di Firenze

MATTEO LONGO Guardia di Finanza
LORENZO MARIA LUCARELLI TONINI Università degli Studi Roma Tre
INDRA MACRÌ Servizio studi della Corte costituzionale
ALESSANDRO MALACARNE Università di Genova
ANTONIO MANGANELLI Università degli Studi di Siena
SOFIA MARCHIAFAVA Sapienza – Università di Roma
ANNALISA MARSANO Autorità garante per la protezione dei dati personali
MARIA LUCE MARINIELLO Autorità per le garanzie nelle comunicazioni (AGCOM)
PILAR MARTÍN RÍOS University of Seville
DARIO MARTIRE Sapienza – Università di Roma
MATTEO MONTI European University Institute – Florence
GAETANA MORGANTE Scuola Superiore Sant'Anna di Pisa
LORENZO NANNIPIERI Istituto di Informatica Giuridica e Sistemi Giudiziari – CNR
CRISTINA NAPOLI Sapienza – Università di Roma
DOMIZIANO PIERANTONI Università degli Studi Roma Tre
MARINA PIETRANGELO Istituto di Informatica Giuridica e Sistemi Giudiziari – CNR
VALERIA PIETRELLA Sapienza – Università di Roma
STEFANO PIETROPAOLI Università degli Studi di Firenze
BENEDETTO PONTI Università degli Studi di Perugia
STEFANIA RACIOPPI Sapienza – Università di Roma
FEDERICA RESTA Autorità Garante per la protezione dei dati personali
FRANCESCA RICCIULLI Università degli Studi Roma Tre
FEDERICO NICCOLÒ RICOTTA Università di Foggia
MILENA ANTONELLA RIZZI Agenzia per la Cybersicurezza Nazionale (ACN)
FEDERICO SERINI Sapienza – Università di Roma
LIVIA SICLARI Università degli Studi Roma Tre
ELISA SORRENTINO Istituto di Informatica e Telematica – CNR
ANNA FEDERICA SPAGNUOLO Istituto di Informatica e Telematica – CNR
GIANCARLO TADDEI ELMI già Istituto di Informatica Giuridica e Sistemi Giudiziari – CNR
SIMONETTA TROZZI Università degli Studi di Perugia
PAOLO ZUDDAS Università dell'Insubria