RIVISTA ITALIANA DI INFORMATICA E DIRITTO

PERIODICO INTERNAZIONALE DEL CNR-IGSG

1•2024

SEZIONE MONOGRAFICA

Il DDL Cybersicurezza (AC1717) Problemi e prospettive in vista del recepimento della NIS2

Instant Book

a cura di Gaia Fiorinelli e Matteo Giannelli

CONTRIBUTI DI

F. Casarosa • P.G. Chiara • G. Fiorinelli
M. Giannelli • G. Morgante • L. Nannipieri
M. Pietrangelo • S. Pietropaoli • F.N. Ricotta
A. Iannuzzi • E. Longo

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

Consiglio Nazionale delle Ricerche

Rivista italiana di informatica e diritto

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 corso della sua storia la Rivista è stata accompagnata da un prestigioso gruppo di corrispondenti stranieri: Y. Amoroso, T.J.M. Bench Capon, D. Bourcier, W.E. Boyd, V. De Mulder, J. Dumortier, F. Galindo, A. Gardner, T. Gordon, G. Greenleaf, O.P. Hance, W. Kilian, F. Lachmayer, P. Leith, E. Mackaay, A. Maclntosh, P. Maharg, J. Mayor, L.T. McCarty, F. Novak, A. Paliwala, A.E. Perez-Luño, R. Petrauskas, L. Philipps, Y. Poullet, A. Saarempaa, E. Schweighofer, P. Seipel, R. Susskind, W.R. Svoboda, H. Yoshino, T. Van Engers, M.A. Wimmer, R. Winkels, J. Zeleznikow.

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

1•2024

Indice

Sezione monografica

Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2 - Instant Book

a cura di Gaia Fiorinelli e Matteo Giannelli

Studi e ricerche

Note e discussioni

Osservatori

*Ri*Leggiamoli

Sezione monografica

Il DDL Cybersicurezza (AC1717)
Problemi e prospettive in vista del recepimento della NIS2

Instant Book

a cura di

Gaia Fiorinelli e Matteo Giannelli

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0151 • articolo non sottoposto a peer review • pubblicato in anteprima il 21 mag. 2024

Gaia Fiorinelli - Matteo Giannelli

Il DDL Cybersicurezza (AC 1717). Problemi e prospettive in vista del recepimento della NIS 2

Introduzione

G. Fiorinelli è ricercatrice in Diritto penale alla Scuola Superiore Sant'Anna di Pisa. M. Giannelli è ricercatore a tempo determinato di Diritto costituzionale nell'Università degli Studi di Firenze

I contributi raccolti in questa sezione monografica della Rivista sono dedicati a una prima analisi dei contenuti del disegno di legge di iniziativa governativa recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" (AC 1717) presentato alla Camera dei deputati in data 16 febbraio 2024.

Gli autori e le autrici dei commenti stanno svolgendo le loro ricerche nell'ambito del Progetto PNRR "Partenariato Esteso" SERICS - *SEcurity and RIghts in the CyberSpace*, finanziato dall'Unione europea - *Next Generation EU*. Proprio nell'ambito di uno degli incontri periodici dello *Spoke 1 – Cyberights*, che vede la partecipazione di sette tra Università e centri di ricerca (Università di Firenze, Milano "Statale", Genova, Bologna, Cagliari, Scuola Superiore Sant'Anna di Pisa e Consiglio Nazionale della Ricerche – CNR), tenuto a Firenze il 26 marzo 2024, è stato affrontato il tema dell'impatto sul nostro ordinamento del disegno di legge 1717, con una serie di interventi dedicati sia al Capo I ("Disposizioni in materia di rafforzamento della cybersicurezza nazionale, resilienza delle pubbliche amministrazioni e del settore finanziario, personale e funzionamento dell'agenzia per la cybersicurezza nazionale, nonché di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici") sia al Capo II del DDL ("Disposizioni per la prevenzione e il contrasto dei reati informatici nonché in materia di coordinamento degli interventi in caso di attacchi a sistemi informatici o telematici e di sicurezza delle banche di dati in uso presso gli uffici giudiziari").

La discussione svolta in quella sede ci ha convinto della necessità, vista l'importanza dei temi trattati, di offrire al dibattito scientifico e istituzionale dei brevi contributi sui numerosi profili affrontati dal testo, mettendoli in relazione con il panorama normativo in materia di cybersicurezza e, in particolare, con il processo che porterà al recepimento della Direttiva (UE) 2022/2555 (c.d. NIS 2), il cui termine scadrà il prossimo 17 ottobre 2024.

L'esame parlamentare svolto in Commissione, che si è avvalso di un cospicuo numero di audizioni informali (due delle quali sono inserite in questa sezione monografica) e di memorie depositate, ha costituito un ulteriore elemento di grande interesse in vista dell'approvazione definitiva e dell'entrata in vigore delle disposizioni.

I contributi pubblicati tengono conto degli emendamenti al testo del DDL votati in sede di Commissione l'8 maggio 2024, delle conseguenti modifiche al testo inizialmente presentato (compresa la nuova numerazione di molte disposizioni) e della successiva approvazione da parte dell'Aula della Camera in data 15 maggio 2024.

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0146 • articolo sottoposto a peer review • pubblicato in anteprima il 17 mag. 2024

FEDERICA CASAROSA

L'armonizzazione degli obblighi di notifica: il DDL Cybersicurezza verso la NIS 2

L'Autrice è tecnologa di ricerca presso la Scuola Universitaria Superiore Sant'Anna e professore presso l'Istituto Universitario Europeo

La ricerca è stata svolta nell'ambito del Progetto PNRR "*SoBigData.it: Strengthening the Italian RI for Social Mining and Big Data Analytics* (CUP B53C22001760006), finanziato dall'Unione europea - Next Generation EU

Questo contributo fa parte della sezione monografica *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2* – Instant Book, a cura di Gaia Fiorinelli e Matteo Giannelli

1. Cybersecurity per la pubblica amministrazione

La sicurezza informatica è stata oggetto dell'attenzione del legislatore italiano sin dai primi anni del 2000, riconoscendo la necessità di un intervento di protezione delle infrastrutture e dei cittadini, ancor prima della c.d. *wake up call* operata a livello europeo dal caso *Wannacry*. Sin dai primi interventi, fra cui il d.lgs. 7 marzo 2005, n. 82 sul codice dell'amministrazione digitale, il legislatore ha mostrato come uno dei primi obiettivi da raggiungere sia l'adeguamento del quadro normativo per il settore pubblico. Anche il DDL Cybersicurezza si pone in questa prospettiva andando a definire strumenti e regole finalizzati a proteggere i soggetti della Pubblica amministrazione che, secondo la recente relazione dell'Agenzia per la Cybersicurezza Nazionale (ACN), sono appunto quelli che hanno subito nel corso del 2023 il numero maggiore di attacchi informatici.

Peraltro, il DDL Cybersicurezza si trova ad intervenire in un momento di transizione, in cui il quadro normativo delineato dal d.lgs. 18 maggio 2018, n. 65, che ha implementato la normativa europea di armonizzazione sulla sicurezza delle reti e dei sistemi informativi (Direttiva n. 2016/1148, c.d. Direttiva NIS) deve essere aggiornato alle nuove regole previste dalla Direttiva 2022/2055, c.d. Direttiva NIS 2. La proposta oggetto dell'analisi, quindi, potrebbe rappresentare un intervento che anticipa alcuni aspetti che saranno poi oggetto della normativa di implementazione della Direttiva NIS 2 e consentire alla Pubblica amministrazione di modificare e adattare le proprie strutture organizzative in tempi adeguati rispetto ai procedimenti interni. Al momento, tuttavia, alcune delle norme previste nella proposta di legge non adottano questa prospettiva, e piuttosto individuano modifiche organizzative che, nel breve periodo, potrebbero a loro volta essere oggetto di ulteriore revisione per allinearsi con le norme previste dalla Direttiva NIS 2.

Uno degli elementi di frizione, su cui si concentra il presente contributo, è relativo agli obblighi di notifica previsti per le Pubbliche amministrazioni in caso di incidente informatico, delineati nell'articolo 1 del DDL Cybersicurezza.

2. Il ruolo degli obblighi informativi nell'attuale quadro normativo

Uno dei pilastri della normativa sulla sicurezza informatica, delineato nella normativa di matrice europea e confluito nella normativa italiana, è quello del rafforzamento della cooperazione strategica fra gli Stati Membri e lo scambio di informazioni attraverso la creazione di un gruppo di cooperazione e di una rete di c.d. "squadre di risposta agli incidenti di sicurezza informatica"(c.d. *Computer Security Incident Response Team* – CSIRT). Tali organismi, predisposti a livello nazionale, hanno il compito di monitorare gli incidenti, fornire un allarme tempestivo in caso di impatto oltre il confine nazionale, avvisare e informare le parti interessate sui rischi e sugli incidenti in corso o avvenuti, rispondere agli incidenti, fornire un'analisi dinamica per aumentare la consapevolezza di tutti gli operatori del mercato. In Italia, questo ruolo viene svolto dall'ACN.

Le informazioni relative agli incidenti sono fornite appunto dagli stessi operatori: gli operatori di servizi essenziali (OSE) sono tenuti a notificare, senza indebito ritardo, gli incidenti che hanno un impatto significativo, rispettivamente sulla continuità e sulla fornitura del servizio, allo CSIRT. Per identificare gli incidenti significativi, gli elementi da valutare sono i seguenti:

- il numero di utenti interessati dall'interruzione di un servizio essenziale;
- l'intervallo di tempo durante il quale il servizio essenziale non è stato operativo;
- l'estensione geografica dell'area interessata dall'incidente.

Il presupposto su cui si basa questo scambio informativo, previsto per la prima volta dalla Direttiva NIS, è il fatto che gli OSE utilizzino sistemi di sicurezza informatica simili nel quadro della loro attività e fornitura di servizi. Ciò significa che l'acquisizione di informazioni relative ad un incidente potrebbe aiutare a scoprire altri incidenti (potenziali o in corso) che coinvolgono altri soggetti che operano nel settore. Dunque, l'analisi degli incidenti potrebbe rivelare vulnerabilità condivise. Questo dimostra che la segnalazione degli incidenti ha un duplice obiettivo: nel breve periodo, mira alla scoperta di attacchi su larga scala e all'identificazione delle vulnerabilità sottostanti al fine di consentire una risposta coordinata agli incidenti, mentre nel lungo periodo, mira ad un miglioramento del livello di sicurezza e di preparazione informatica.

È da sottolineare, tuttavia, che la Direttiva NIS, fa riferimento ad una indicazione temporale indefinita per quanto riguarda i tempi di notifica, poiché richiede l'invio della segnalazione "senza indebito ritardo". Questa generica indicazione è stata poi tradotta in un procedimento ben delineato nel d.P.C.M. 14 aprile 2021, n. 81 che prevede una differenziazione sulla base dell'impatto degli incidenti relativi alla sicurezza informatica sugli *asset* ICT degli enti inclusi nel c.d. Perimetro di Sicurezza Nazionale Cibernetico (PSNC - definito con il d.l. 21 settembre 2019, n. 105, DL Perimetro). La tassonomia prevista distingue due tipologie di incidenti sulla base della gravità dello stesso: la Tabella 1 dell'Allegato A contiene gli incidenti meno gravi (e.g. infezione, guasto, installazione, movimenti laterali, azioni sugli obiettivi) e la Tabella 2 quelli più gravi (e.g. azioni sugli obiettivi e disservizio). Questa classificazione è funzionale alle diverse tempistiche necessarie per una risposta efficace. Pertanto, gli OSE dovranno riferire al CSIRT italiano entro un'ora nel caso di un incidente identificato nella Tabella 2 e sei ore nel caso di un incidente rientrante nella Tabella 1. Tali termini decorrono dal momento in cui l'ente viene a conoscenza dell'incidente, ad esempio attraverso le attività di monitoraggio, test e controllo svolte sulla base delle misure di *cybersecurity* previste dallo stesso decreto.

Se l'ente viene a conoscenza di nuovi elementi significativi, tra cui specifiche vulnerabilità sfruttate o, più in generale, la rilevazione di eventi in qualche modo correlati all'incidente, la notifica deve essere modificata senza indebito ritardo dal momento in cui se ne viene a conoscenza, a meno che l'autorità giudiziaria non abbia precedentemente richiesto specifiche esigenze di segretezza delle indagini (si veda l'art. 3(5) d.P.C.M. 81/2021). Inoltre, su richiesta del CSIRT, l'ente che ha notificato un incidente è tenuto, entro sei ore dalla richiesta, ad aggiornare la notifica, ad eccezione dei casi in cui sussistano specifiche esigenze di segreto investigativo.

Ai precedenti obblighi sono aggiunti quelli previsti per gli incidenti che hanno un impatto su reti, sistemi informativi e servizi informatici che si trovano al di fuori del PNSC (diversi quindi dai menzionati asset ICT) ma che sono di pertinenza

di soggetti inclusi nel PNSC (previsti dal novellato art. 1(3-*bis*) del DL Perimetro, così come introdotto dall'art. 37-*quater* (1) d.l. 9 agosto 2022, n. 115, convertito, con modificazioni, in legge 21 settembre 2022). Tali obblighi hanno un termine di notifica di 72 ore; pertanto, meno stringente rispetto a quelli previsti per i beni Perimetro, ma che per limitare eventuali duplicazioni prevede una tassonomia degli incidenti equivalente a quella prevista nelle Tabelle A e B del d.P.C.M. 81/2021 e modalità di notifica in linea con quelle già esistenti.

3. Le novità che emergono dalla Direttiva NIS 2

La Direttiva NIS 2 cerca di superare alcuni dei limiti che erano emersi dall'implementazione della precedente Direttiva NIS. In particolare, sono modificati i criteri per l'identificazione dei soggetti inclusi nel campo di applicazione, passando dalla distinzione fra OSE e fornitori di servizi digitali alla distinzione tra i cosiddetti enti essenziali (*essential entities* - EE) ed importanti (*important entities* - IE). La distinzione non è giustificata da un diverso insieme di requisiti e obblighi di notifica, come accadeva nella direttiva NIS, ma riguarda soltanto il tipo di meccanismi di sorveglianza applicati. Inoltre, la direttiva estende lo scopo di applicazione agli enti della Pubblica amministrazione, prevedendo un obbligo per le strutture centrali e lasciando un livello di discrezionalità agli Stati membri su quella locale (art. 2(f) Direttiva NIS 2). È da sottolineare che le pubbliche amministrazioni non erano escluse dallo scopo di applicazione della Direttiva NIS; tuttavia, rientravano soltanto quelle identificate come OSE dai singoli Stati Membri (considerando (45) Direttiva NIS).

Anche gli obblighi di notifica sono oggetto di modifica e la Direttiva NIS 2 distingue due fasi per la segnalazione degli incidenti. Durante la prima fase, l'entità interessata deve informare, con un rapporto iniziale, lo CSIRT entro ventiquattro ore da quando venga a conoscenza di un incidente. Successivamente, lo stesso soggetto fornirà un rapporto completo entro settantadue ore da quando sia venuto a conoscenza dell'incidente. La seconda fase riguarda il ripristino completo del problema, con la presentazione di un rapporto finale ad un mese dopo il rapporto iniziale.

Si noti che la segnalazione di incidenti cd. significativi è obbligatoria, mentre per qualsiasi altro incidente di livello inferiore non è necessaria la notifica. Tuttavia, al fine di acquisire un quadro completo del panorama delle minacce, la normativa europea fornisce una base giuridica per le notifiche volontarie di incidenti significativi, minacce informatiche e quasi incidenti da parte di entità che non rientrano nell'ambito di applicazione, lasciando agli Stati membri la scelta di dare priorità al trattamento delle notifiche obbligatorie rispetto a quelle volontarie (art. 29 Direttiva NIS 2).

4. Gli obblighi informativi nel DDL Cybersicurezza

Gli obblighi di segnalazione previsti dal DDL Cybersicurezza mostrano una netta differenza dalle norme previste dal d.P.C.M. 81/2021 e una parziale convergenza con le norme previste dalla Direttiva NIS 2. Ai sensi dell'art. 1, le pubbliche amministrazioni sono tenute a segnalare gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici previsti nella tassonomia indicata dall'art. 1 (3-*bis*) d.l. 105/2019. La segnalazione deve essere effettuata entro ventiquattro ore dal momento in cui i soggetti sono venuti a conoscenza dell'evento, cui segue una successiva notifica di tutti gli elementi disponibili entro settantadue ore.

Se approvato secondo il testo attuale, le pubbliche amministrazioni potrebbero trovarsi - nelle more dell'implementazione della Direttiva NIS 2 – a dover valutare se ricadano in una delle seguenti ipotesi. In un primo caso, la Pubblica amministrazione potrebbe essere inclusa nel PNSC e dunque sottoposta al regime previsto dal d.P.C.M. 81/2021. Nel caso in cui l'incidente abbia ad oggetto gli *asset* ICT, la Pubblica amministrazione è tenuta a notificare l'incidente entro un'ora o sei ore dal momento in cui è venuta a conoscenza dell'evento; invece, laddove l'incidente ha ad oggetto reti, sistemi informativi e servizi informatici di pertinenza delle Pubbliche amministrazioni, i tempi si allungano fino a settantadue ore dal momento in cui sono venuti a conoscenza dell'evento. In un secondo caso, la Pubblica amministrazione non è inclusa nel PNSC, ma ricade nelle categorie previste dall'art. 1(1) DDL Cybersicurezza. In caso di incidente che abbia ad oggetto reti, sistemi informativi e servizi informatici (equivalenti ai sopramenzionati *asset* ICT), la Pubblica amministrazione è tenuta a segnalare l'incidente entro ventiquattro ore ed a fornire tutti gli elementi disponibili entro

settantadue ore. Sia nella prima che nella seconda ipotesi, la Pubblica amministrazione non è tenuta a successivi aggiornamenti in merito alla risoluzione dell'incidente.

Indipendentemente dal fatto l'inclusione nel PNSC è segreto di stato, appare evidente che i termini per la segnalazione sono variegati e portano ad una frammentazione che influisce negativamente sull'obiettivo di una rapida e coordinata risposta rispetto ad un eventuale incidente. Da un lato, dal combinato disposto emerge la necessità di un intervento di armonizzazione che permetta alle amministrazioni di rispondere con celerità agli incidenti semplificando il meccanismo di segnalazione in linea con i termini previsti con la Direttiva NIS 2. Dall'altro lato, la mera comunicazione dell'incidente senza una successiva fase di verifica del contenimento e della risoluzione dell'attacco informatico non permette di raggiungere l'obiettivo di una maggiore consapevolezza circa i rischi e le buone pratiche che possono portare al miglioramento del livello di sicurezza a livello generale. Questo passaggio ulteriore è già previsto dalla Direttiva NIS 2, che richiede una seconda fase di aggiornamento ad un mese dalla prima segnalazione. In questo senso, potrebbe essere auspicabile dunque una revisione del testo attuale in cui sia previsto tale ulteriore indicazione, che anticiperebbe l'implementazione della normativa europea e porterebbe ad incrementare i livelli di sicurezza attraverso un maggiore scambio di informazioni.

Riferimenti bibliografici

Agenzia per la Cybersicurezza Nazionale (2023), *Relazione Annuale al Parlamento*, 2023

F. Casarosa, G. Comandé (2024), *Aspettando la NIS2: ovvero il diritto privato della cybersecurity*, in "Diritto dell'informazione e dell'informatica", 2024, n. 1

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)*, in "Rivista italiana di informatica e diritto", 2024, n. 1

S. Rossa (2023), *Cyber attacchi e incidenti nella pubblica amministrazione, fra organizzazione amministrativa e condotta del funzionario*, in "Vergentis: revista de investigación de la Cátedra Internacional conjunta Inocencio III", 2023, n. 17

S. Schmitz-Berndt (2023), *Defining the Reporting Threshold for a Cybersecurity Incident under the NIS Directive and the NIS 2 Directive*, in "Journal of Cybersecurity", vol. 9, 2023, n. 1

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0145 • articolo sottoposto a peer review • pubblicato in anteprima il 17 mag. 2024

Matteo Giannelli

Il contributo dei livelli di governo substatali al raggiungimento degli obiettivi del ddl Cybersicurezza

L'Autore è ricercatore a tempo determinato di Diritto costituzionale nell'Università degli Studi di Firenze

La ricerca è stata svolta nell'ambito del Progetto PNRR "Partenariato Esteso" *SERICS - SEcurity and RIghts in the CyberSpace, Spoke 1 – Cyberights* (CUP B83C22004830007), finanziato dall'Unione europea - Next Generation EU

Questo contributo fa parte della sezione monografica *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2* – Instant Book, a cura di Gaia Fiorinelli e Matteo Giannelli

1. Il disegno di legge di iniziativa governativa recante *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici* (A.C. 1717) in discussione presso la Camera dei deputati ha l'obiettivo di consolidare sia la risposta penale alle minacce alla sicurezza informatica quanto la resilienza della pubblica amministrazione. Sotto quest'ultimo profilo le disposizioni contenute nel testo rispondono a due necessità che si sono manifestate sempre di più negli ultimi anni: da un lato, far emergere in modo puntuale e tempestivo la minaccia informatica diretta ai soggetti della pubblica amministrazione non compresi nel Perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge 21 settembre 2019, n. 105; dall'altro, costituire una sorta di anticipazione a livello nazionale in vista dell'attuazione nel nostro ordinamento della Direttiva (UE) 2022/2555 (c.d. NIS 2), il cui termine per il recepimento da parte degli Stati membri scadrà il prossimo 17 ottobre 2024.

Sul punto occorre preliminarmente ricordare che ai sensi dell'art. 2, par. 5, della Direttiva, le nuove disposizioni si applicano agli enti della pubblica amministrazione a livello centrale, mentre in sede di attuazione i singoli Stati membri decideranno se estenderle anche agli enti a livello regionale e locale. Completano il quadro i paragrafi 6 e 7 del medesimo articolo che, rispettivamente, lasciano impregiudicata la responsabilità degli Stati membri di tutelare la sicurezza nazionale e il loro potere di salvaguardare altre funzioni essenziali dello Stato e prevedono l'esclusione degli 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.

Da questa breve rassegna normativa dovrebbe risultare evidente come l'attuazione della Direttiva comporti moltissimi problemi di coordinamento, che possono minare l'efficacia e il risultato atteso dal legislatore europeo e nazionale. Problemi, in una certa misura inevitabili poiché strettamente connessi ai fenomeni di integrazione – non solo

normativa – tra ordinamenti ma che devono esser messi in luce con la dovuta attenzione. In questo breve contributo verranno affrontati, sia consentito l'utilizzo del termine, solamente quelli verso "il basso" (riferiti dunque ai livelli di governo substatali) e, almeno direttamente, non quelli "verso l'alto" (riferiti al tema della sicurezza nazionale e alle sue declinazioni).

2. Le disposizioni contenute nel Capo I si inseriscono nel variegato panorama normativo concernente i temi della sicurezza informatica e dello spazio digitale nel nostro ordinamento, attraverso una serie di misure appositamente congegnate per garantire la resilienza intesa quale capacità di una rete o di un sistema di mantenere la funzionalità e di adattarsi, preservando le proprie caratteristiche, in risposta ad attacchi, perturbazioni o crisi in coordinamento con le autorità competenti. Un panorama che si comporrà definitivamente con l'entrata in vigore dei decreti delegati previsti dell'articolo 3 della legge 21 febbraio 2024, n. 15, "Legge di delegazione europea" e che, come detto, dovranno essere emanati entro il 17 ottobre 2024 con riferimento al recepimento della Direttiva NIS 2.

Nel definire il contenuto di tali decreti il Governo, in raccordo con l'Agenzia per la Cybersicurezza Nazionale (ACN), dovrà «individuare i criteri in base ai quali un ente pubblico può essere considerato pubblica amministrazione ai fini dell'applicazione delle disposizioni della direttiva (UE) 2022/2555, anche considerando la possibilità di applicazione della direttiva medesima ai comuni e alle province secondo principi di gradualità, proporzionalità e adeguatezza» (art. 3, co. 1, lett. a). Dovrebbe a questo punto risultare chiaro il collegamento con il ddl in commento e, in particolare con gli articoli 1, 2, 8 e 13, che, occupandosi anche dei livelli regionali e locali, chiedono al legislatore una visione d'insieme per evitare che nuove disposizioni e i connessi obblighi rimangano sulla carta o, ipotesi peggiore, si risolvano in un fattore di confusione dell'intero sistema.

Una consapevolezza che sembra confermata dalla lettura nell'analisi tecnico-normativa dell'A.C. 1717 (supplemento, pag. 15) dove alla voce *Analisi delle compatibilità dell'intervento con le competenze e le funzioni delle regioni ordinarie e a statuto speciale nonché degli enti locali* è possibile leggere che «le disposizioni proposte con il Capo I del presente disegno di legge rientrano tra le materie riservate in via esclusiva allo Stato e, in particolare, tra quelle indicate dall'articolo 117, secondo comma, lettera d), della Costituzione. Non si ravvisano, pertanto, profili di incompatibilità con le competenze e le funzioni delle regioni ordinarie e a statuto speciale, nonché degli enti locali. Tuttavia, in considerazione della incidenza di talune disposizioni previste dal provvedimento – in particolare, gli articoli 1, 2, 6 e 10 – sulle attività delle pubbliche amministrazioni anche locali, sarà necessario un confronto ed un raccordo operativo con i richiamati soggetti in relazione all'attuazione di tali disposizioni». Ancora alla successiva voce *Verifica della compatibilità con i principi di sussidiarietà, differenziazione ed adeguatezza sanciti dall'articolo 118, primo comma, della Costituzione* si legge che «le disposizioni contenute nell'intervento esaminato sono compatibili e rispettano i principi di cui all'articolo 118 della Costituzione, in quanto non prevedono né determinano, sia pure in via indiretta, nuovi o più onerosi adempimenti a carico degli enti locali».

Dalla prima affermazione appena riportata sembra emergere chiaramente, specie dal periodo conclusivo, un comune consenso in merito alla circostanza che l'imposizione agli enti locali e regionali di vincoli in materia di cybersicurezza, implichi necessariamente un coordinamento e un concreto supporto volto alla realizzazione di condizioni effettive di resilienza cibernetica. Qualche perplessità si ricava, invece, dalla seconda voce soprattutto con riferimento all'assenza di oneri indicata nella parte finale e che sembra ignorare che uno dei problemi principali della cybersicurezza è quello dei costi, non solo sotto il profilo degli attacchi e delle loro conseguenze ma anche sotto quello, preliminare – o meglio preventivo – della *compliance* dei soggetti pubblici e privati.

3. A questo punto occorre chiedersi in che modo il testo delle disposizioni del ddl rilevanti ai fini della presente trattazione intendono affrontare e risolvere le questioni emerse. L'art. 1 nel prevedere un più ampio obbligo di notifica di incidenti rilevanti per la cybersicurezza per soggetti ulteriori rispetto a quelli già ricompresi nel perimetro di sicurezza nazionale cibernetica e l'articolo 8 nell'occuparsi del rafforzamento della resilienza delle pubbliche amministrazioni e dell'individuazione del referente per la cybersicurezza sembrano trascurare una fattiva collaborazione con gli enti locali e regionali. Una cooperazione che si dovrebbe basare

sul modello CSIRT (*Computer Security Incident Response Team*) – oggetto di parziale intervento nell'articolo 21 – che, ad oggi, costituisce l'ambito privilegiato per identificare i problemi, per offrire una risposta coordinata agli incidenti informatici, per realizzare uno scambio di buone pratiche – come sollecitato in più punti anche dalla Direttiva NIS 2 a partire dell'art. 15 – e, in definitiva, incentivare il rispetto delle disposizioni in materia.

Sembra mancare un riferimento alla possibilità per le Regioni e le province autonome, sulla base di accordi con l'Agenzia per la cybersicurezza nazionale, di istituire CSIRT regionali operanti in raccordo con lo CSIRT nazionale. Una previsione che, peraltro, sarebbe in linea con quanto previsto nella Strategia Cyber nazionale e nelle progettualità in ambito PNRR (Misura 1 investimento 1.5), che prevedono appunto l'istituzione di CSIRT di livello regionale, come sta avvenendo in alcuni contesti territoriali, anche grazie al contributo dei diversi enti, anche non territoriali (si pensi ad esempio al contributo delle Università). Inoltre, l'organizzazione e le attività degli CSIRT regionali costituendo elementi di carattere strategico dovrebbero essere oggetto di intesa in sede di Conferenza Stato-Regioni per garantire la massima condivisione tra livello centrale e livello periferico e favorire meccanismi di raccordo con le Regioni da parte dell'Agenzia per la Cybersicurezza Nazionale ad oggi molto limitati.

In termini più generali, l'impianto delle disposizioni appare analogo ad altre che presentano il classico schema adempimento-sanzione. Una circostanza auto evidente nel Capo II per il versante penalistico ma riscontrabile anche nel capo I, quasi a testimoniare la preminenza di un modello sull'altro a scapito di una concezione (anche) promozionale della sicurezza nel modo digitale. Si tratta di un approccio che si scontra con l'esigenza operativa di intervento richiesta dalle norme in materia di cybersicurezza e, di conseguenza, con la successiva messa in atto degli adempimenti. L'introduzione di un Referente per la cybersicurezza in ogni Amministrazione dimostra un'attenzione alle nuove sfide presentate dalla disciplina anche se, tuttavia, la semplice presenza di figure di riferimento, peraltro in assenza di una chiara definizione del loro livello di inquadramento, non appare sufficiente a garantire i risultati. Diviene, dunque, fondamentale che il livello a centrale, a partire dall'Agenzia per la Cybersicurezza Nazionale, oltre a introdurre novità normative, lavori a stretto contatto con i Referenti nelle varie amministrazioni per garantire che i compiti pianificati siano effettivamente realizzati e che vi sia un chiaro processo di monitoraggio e valutazione dei risultati ottenuti, affiancandoli nell'implementazione di strategie operative e di procedure. In coerenza con l'obiettivo di rendere la cybersicurezza una priorità, vista la natura trasversale e pervasiva della stessa rispetto alla ormai totalità dei servizi di funzionamento delle amministrazioni, ai processi digitalizzati e ai servizi erogati, dovranno esser adottate misure in grado di incidere efficacemente e tempestivamente. Tra le ipotesi, potrebbero esser introdotti pareri obbligatori da parte del Referente per la cybersicurezza su diverse categorie di atti dell'ente e la possibilità di emanare linee guida e raccomandazioni interne, in coordinamento con gli organi previsti dalla normativa vigente.

La configurazione della figura del Referente che si ricava dall'art. 8 sembra essere difficilmente conciliabile con questa impostazione. Sullo sfondo di questa vicenda non bisogna dimenticare le crescenti difficoltà delle amministrazioni nel reclutare specialisti ICT dotate di competenze avanzate specifiche in ragione di una diffusa carenza nel mercato, non solo pubblico ma anche privato, delle competenze ICT e, in particolare, di formazione nel campo della cybersicurezza. Una circostanza che potrebbe tradursi in una potenziale criticità nell'individuazione delle risorse umane previste dall'articolo 8, comma 1 e 2, e che potrebbe comportare, come avvenuto per i Responsabili per la Transizione digitale (RTD) di cui Decreto legislativo 7 marzo 2005 n. 82 (Codice dell'Amministrazione Digitale – CAD), l'individuazione di personale privo delle necessarie competenze e un conseguente mancato rafforzamento delle Amministrazioni.

Una lacuna a cui si è posto parzialmente rimedio attraverso alcune modifiche al testo apportate in sede referente dalle Commissioni riunite Affari Costituzionali e Giustizia. Al fine di agevolare in particolare gli enti di minori dimensioni o quelli che utilizzano sistemi informativi erogati dalle società in house o dalla Regione come soggetto aggregatore, è stata introdotta la possibilità che il ruolo di referente sia svolto da un dipendente di un'altra pubblica amministrazione nel caso in cui non vi siano dipendenti dotati specifiche

professionalità e competenze (comma 2) oppure che sia possibile una nomina associata (comma 4), in analogia a quanto previsto dall'art. 17, comma 1-*septies* del citato CAD che prevede anche la possibilità di esercitare le funzioni di RTD in forma associata. Tale previsione, peraltro, potrebbe rispondere all'ampliamento dell'ambito soggettivo di applicazione della Direttiva 2022/2555 NIS 2 con riferimento ai soggetti pubblici. Di ulteriore interesse è il comma 5, anch'esso introdotto in sede referente, che attribuisce all'Agenzia per la Cybersicurezza Nazionale la possibilità di individuare le modalità e i processi di coordinamento e collaborazione, anche di livello regionale, tra le amministrazioni individuate all'articolo 1, comma 1, e i referenti appena descritti al fine di facilitare la resilienza delle amministrazioni pubbliche.

Nella direzione di un difficile coordinamento in fase di risposta alle minacce sembra muoversi l'articolo 2, comma 1, del ddl quando prevede che le amministrazioni, gli enti pubblici e altri soggetti che forniscono servizi pubblici, qualora siano oggetto di segnalazioni dell'Agenzia per la cybersicurezza nazionale circa specifiche vulnerabilità cui essi risultano potenzialmente esposti, debbano provvedere tempestivamente all'adozione degli interventi risolutivi indicati dalla stessa Agenzia. Dal momento che tale previsione prevede applicazione di sanzioni per inadempimento, l'utilizzo del termine "potenzialmente" sembra rischioso per la concreta possibilità di far ricadere in questa fattispecie non solo segnalazioni puntuali proveniente dall'Agenzia ma anche quelle su cui non ci sono, e non sono verificabili, effettive evidenze di rischio da parte del soggetto pubblico che riceve tale segnalazione.

Un'ultima postilla riguarda la previsione, apparentemente marginale, contenuta nell'articolo 11, comma 1, dove sono definiti tempi e modalità per l'adozione del regolamento che stabilisce termini e disposizioni operative per l'accertamento, la contestazione e la notificazione delle violazioni della normativa in materia di cybersicurezza e l'irrogazione delle relative sanzioni di competenza dell'Agenzia. Nella disposizione si precisa che il regolamento può essere adottato «anche in deroga all'art. 17 della legge 23 agosto 1988, n. 400». Quest'ultimo inciso è stato introdotto in sede referente e sarà solo la prassi a dimostrarne l'efficacia, anche se in situazioni analoghe tale previsione non è apparsa sufficientemente apprezzabile. Sul punto è possibile in termini generali osservare che la deroga al procedimento di formazione dei regolamenti previsto in via generale dall'art. 17 della legge 400 del 1988 possa costituire, come avvenuto in particolare a partire dalla Riforma del Titolo V, una potenziale fattore contrastante il riparto di competenze tra Stato e Regioni previsto dall'articolo 117, comma 6, della Costituzione.

Riferimenti bibliografici

E. Longo (2024), La disciplina della Cybersicurezza nell'Unione europea e in Italia, in F. Pizzetti et al. (a cura di), "La regolazione europea della società digitale", Giappichelli, 2024

S. Poletti (2023), *La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica*, in "MediaLaws", 2023, n. 2

S. Rossa (2023), *Cybersicurezza e Pubblica Amministrazione*, Editoriale Scientifica, 2023

R. Ursi (2023), *La sicurezza cibernetica come funzione pubblica*, in Id. (a cura di), "La sicurezza nel cyberspazio", FrancoAngeli, 2023

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0149 • articolo sottoposto a peer review • pubblicato in anteprima il 17 mag. 2024

Lorenzo Nannipieri

Cybersicurezza e appalti pubblici: verso un nuovo (e incerto) quadro regolatorio

L'Autore è ricercatore presso l'IGSG/CNR

Questo contributo fa parte della sezione monografica *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2* – Instant Book, a cura di Gaia Fiorinelli e Matteo Giannelli

1. L'art. 10 del DDL 1717 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».

Nello spirito dell'iniziativa legislativa, come risultante dalla relazione tecnica al DDL, le disposizioni proposte mirerebbero a promuovere maggiore garanzia delle esigenze di cybersicurezza nelle ipotesi in cui le attività di approvvigionamento delle PP.AA. siano connesse alla tutela degli interessi nazionali strategici.

Prima di esaminare il contenuto dell'articolo, occorre premettere che le disposizioni devono essere lette nel quadro normativo vigente in seguito all'entrata in vigore del nuovo codice dei contratti pubblici (d.lgs. 31 marzo 2023, n. 36) e, segnatamente, delle novità introdotte dall'art. 108 del codice stesso.

Quest'ultima disposizione, nel regolamentare l'aggiudicazione di appalti, servizi e forniture sulla base del criterio dell'offerta economicamente più vantaggiosa, prevede (comma 4) che gli «elementi di cybersicurezza» debbano costituire un contenuto indefettibile dei documenti di gara nella scelta in ordine ai criteri di aggiudicazione dell'offerta ritenuti maggiormente pertinenti rispetto alla natura, all'oggetto e alle caratteristiche del contratto e al fine di individuare il miglior rapporto qualità prezzo per l'aggiudicazione.

L'esame della disposizione codicistica – pur problematica, sotto vari aspetti – esula dall'oggetto del presente contributo, ai fini del quale appare però necessario ricordare che il codice ha posto a carico delle stazioni appaltanti un generale obbligo di «considerazione» degli aspetti legati alla cybersicurezza, che subisce un aggravamento (invero piuttosto imprecisato) negli ambiti in cui l'attività appaltata intercetta gli interessi nazionali strategici.

Le misure adottate (o proposte) dal legislatore italiano si collocano nell'ambito della complessiva strategia nazionale per la cybersicurezza secondo cui «ogni Stato membro adotta una strategia nazionale per la cybersicurezza che prevede gli obiettivi strategici e le risorse necessarie per

conseguirli, nonché adeguate misure strategiche e normative al fine di raggiungere e mantenere un livello elevato di cybersicurezza» (Direttiva NIS 2, art. 7, comma 1).

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).

2. Il primo comma dell'art. 10 prevede – oggi divenuto art. 13 nella versione attualmente in esame, comprensiva degli emendamenti approvati durante l'esame in commissione in sede referente nella sessione dell'8 maggio 2024 – che «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 di cui all'articolo 5 della legge 3 agosto 2007, n. 124, nella composizione di cui all'articolo 10, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, 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). Ai fini del presente articolo, per «elementi essenziali di cybersicurezza» si intende 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».

Sul piano oggettivo, la disposizione 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 non riferibile 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 del (già vigente) art. 108, co. 4, d.lgs. 36/2023, già richiamato nelle premesse.

Problematica, però, è l'individuazione di un concetto positivo di «interesse nazionale strategico», ricorrente sia nel DDL 1717 che nel codice.

Sul punto, il DDL 1717 parrebbe operare un rimando implicito agli artt. 5 e 7 del d.l. 82/2021 che, nell'istituire l'ACN, ne 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. 15 marzo 2012, n. 21, recante «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. 5 dicembre 2022, n. 187, recante «misure urgenti a tutela dell'interesse nazionale nei settori produttivi strategici»).

Quello che parrebbe 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 (per una definizione di «funzione essenziale dello stato», parzialmente affine a quella di «interesse nazionale strategico», si rinvia all'art. 2, co. 1, lett. a), d.P.C.M. 30 luglio 2020, n. 131, 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»).

Allo stato attuale, specialmente in considerazione della grande proliferazione di norme di rango primario e regolamentare, sembra esistere effettivamente un problema tassonomico/definitorio, 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 deflattive.

La seconda nozione che delimita l'ambito oggettivo di applicazione dell'art. 10 è quella di «elementi essenziali di cybersicurezza», dizione ricorrente, anch'essa, nel già citato art. 108, co. 4, del d.lgs. 36/2023.

Rispetto a quest'ultima disposizione, l'art. 108 DDL 1717 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».

Si tratta di un tentativo da apprezzare positivamente, atteso che l'intervento pare colmare una lacuna lasciata dalla formulazione piuttosto vaga dell'art. 108, comma 4, d.lgs. 36/2023 che, in effetti, nel riferirsi agli «elementi di cybersicurezza» non ne ha sufficientemente circoscritto l'ambito definitorio.

Rimane ferma, però, l'esigenza di distinguere gli «elementi essenziali di cybersicurezza» dagli «elementi di cybersicurezza» di cui all'art. 108 del codice, atteso che il requisito dell'essenzialità (presente nell'art. 10 in commento ma non nell'art. 108, comma 4, del codice) appare, a propria volta, un concetto sfuggente e di difficile delimitazione.

L'ambito soggettivo di applicazione dell'art. 10 del DDL si desume dal combinato disposto dell'art. 10, comma 1, del DDL 1717, da un lato e, dall'altro lato, gli artt. 2 d.lgs. 82/2005 (Codice dell'amministrazione digitale) e 1, comma 2, d.lgs. 30 marzo 2001, n. 165 (T.U.P.I.) individuando, quali destinatari, i seguenti soggetti:

1. 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, 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 d.lgs. 30 luglio 1999, n. 300;
2. autorità di sistema portuale;
3. autorità amministrative indipendenti di garanzia, vigilanza e regolazione;
4. gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse;
5. società a controllo pubblico, con esclusione delle società quotate.

Questo elenco di destinatari delle disposizioni in materia di appalti pubblici contenute nel DDL 1717 appare decisamente ampio.

Come osservato in sede istruttoria (cfr. audizione dell'ANCI), l'ambito di applicazione della disposizione dovrebbe essere meglio specificato, in quanto il rinvio *per relationem* all'art. 2, co. 2, d.lgs. 82/2005 condurrebbe ad una generalizzata efficacia applicativa della disposizione anche a soggetti che non svolgono attività di approvvigionamento di beni e servizi informatici legati alla tutela di interessi nazionali strategici.

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 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. 21 settembre 2019, n. 105.

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, è istituito il perimetro di sicurezza nazionale cibernetica» (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).

3. Il secondo comma dell'art. 10 del DDL 1717 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.

Dal punto di vista sistematico, la disposizione avrebbe trovato una migliore collocazione nell'art. 108 del codice e non in un testo normativo ad esso estraneo.

Il rinvio all'art. 107, comma 2, d.lgs. 36/2023, appare frutto di una tecnica normativa di dubbia apprezzabilità, atteso che la citata disposizione codicistica è riferita a vizi dell'offerta attinenti a fattori del tutto distinti dalla cybersicurezza (obblighi in materia ambientale, sociale e del lavoro), circostanza che renderebbe opportuna, semmai, una revisione dello stesso art. 107, comma 2, del codice ovvero del successivo art. 108, piuttosto che l'inserimento in un distinto provvedimento normativo di una disposizione che, di fatto, ne allarghi l'ambito applicativo.

Inoltre, per quanto l'intera disposizione avrebbe trovato una miglior collocazione sistematica altrove, il «gancio» normativo con le facoltà di cui all'art. 108, comma 10, del codice (non aggiudicazione dell'appalto in caso di inidoneità di tutte le offerte rispetto all'oggetto del contratto) appare congruo in quanto il rinvio è riferito, in questo caso, ad una disposizione codicistica formulata in termini generali.

Al punto b), il comma 2 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».

La disposizione appare 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».

Stesso dicasi per la lettera d), secondo cui 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». La disposizione sembra ricalcare pedissequamente quanto già previsto dall'art. 108, comma 4, penultimo periodo, del codice, nella parte in cui è specificato 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».

In sede di esame in commissione, è stato approvato un emendamento con cui si è proposto di aggiungere una lettera d-bis), secondo cui le Stazioni Appaltanti «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, al fine di tutelare la sicurezza nazionale e di conseguire l'autonomia tecnologica e strategica nell'ambito della cybersicurezza».

Innovativa, invece, appare la previsione della lettera c), che introduce 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, ll DDL 1717 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, l'implementazione – *de facto* – della portata prescrittiva dell'art. 108 del codice parrebbe foriera del rischio di apportare un deciso aggravio in termini di contenzioso amministrativo, specialmente per il carattere non sufficientemente delineato della nozione di «interessi nazionali strategici», dei diversi adempimenti che gli operatori sarebbero chiamati a rispettare in punto di cybersicurezza (elementi «essenziali» o meno di cybersicurezza, a seconda dei casi) e della latitudine della discrezionalità riservata alle Stazioni appaltanti per la valutazione delle offerte in punto di adempimenti cyber.

Ancor più critica, sul piano sistematico, è la previsione di cui al comma 4, nella versione riformulata con una proposta emendativa approvata durante l'esame in commissione in sede referente, secondo cui «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».

Al di là del merito della questione, risulta piuttosto sfuggente la logica di introdurre una disposizione normativa di rango primario finalizzata a «mantenere ferma» un'altra norma di pari rango, mai abrogata.

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0142 • articolo sottoposto a peer review • pubblicato in anteprima il 17 mag. 2024

Marina Pietrangelo

Per un modello nazionale di cybersicurezza cooperativa e resilienza collaborativa

L'Autrice è prima ricercatrice presso l'IGSG/CNR

Questo contributo fa parte della sezione monografica *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2* – Instant Book, a cura di Gaia Fiorinelli e Matteo Giannelli

1. Premessa

Il disegno di legge AC 1717 *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici* d'iniziativa governativa (Presidente del Consiglio Meloni e Ministro della Giustizia Nordio) è stato depositato alla Camera dei deputati il 16 febbraio 2024 ed è attualmente all'esame di merito delle Commissioni riunite Affari costituzionali e Giustizia. La proposta interviene su un quadro regolatorio complesso, risultato della stratificazione di numerose fonti interne ed eurounionali, e prossimo ad essere ulteriormente novellato dalla *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 (cosiddetta "direttiva NIS 2")*. La delega per l'adozione del decreto legislativo di recepimento della NIS 2 è nella legge di delegazione europea 2022-2023 (cfr. l'art. 3, l. 21 febbraio 2024, n. 15, *Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2022–2023)*. Di tale direttiva – che ha innovato significativamente le norme pregresse e di cui si attende il recepimento in ottobre – il disegno di legge governativo anticipa alcune misure, senza tuttavia prevedere forme di raccordo con essa. L'intervento proposto risulta quindi asincrono, e rischia di produrre ulteriore incertezza.

2. Sui tratti generali del ddl

A prima lettura, il progetto legislativo sembra presentare più d'una criticità tanto sotto il profilo sostanziale, che sconfina inevitabilmente ben oltre la cybersicurezza in senso stretto (che è «l'insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche», secondo la definizione dell'art. 1, co. 1, n. 1, *Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, 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; ripresa in art. 1, co. 1, lett. a), *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*, conv. con modifiche nella legge n. 109/2021), che sotto quello parimenti rilevante – e al primo strettamente embricato – del modello regolatorio.

La proposta è costruita attorno a due distinte aree di intervento: la prima insiste specialmente sulla cybersicurezza delle amministrazioni pubbliche e sulla governance di settore; la seconda contiene misure di carattere penale. La prima coincide col Capo I (artt. 1-10) intitolato "Disposizioni in materia di rafforzamento della cybersicurezza nazionale, resilienza delle pubbliche amministrazioni, personale e funzionamento dell'Agenzia per la cybersicurezza nazionale. Nonché di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici"; la seconda col Capo II (artt. 11-18) recante "Disposizioni per la prevenzione e il contrasto dei reati informatici nonché in materia di coordinamento degli interventi in caso di attacchi ai sistemi informatici e telematici".

Nel paragrafo successivo saranno esaminate più in dettaglio alcune disposizioni del Capo I, che potrebbero porre problemi sotto il profilo della sostenibilità amministrativa e più in generale in termini di leale collaborazione tra gli enti interessati dalla nuova normativa. Prima però di addentrarci nello specifico di queste previsioni, qualche notazione di carattere generale. Anzitutto, l'articolato nel suo complesso tradisce l'idea di un irrobustimento della cybersicurezza che si esprime attraverso una verticalizzazione della relativa governance, con un ulteriore accentramento di poteri e funzioni nell'apparato governativo dello Stato. A tenore della proposta, infatti, l'endiadi legislativa "sicurezza e resilienza" delle amministrazioni pubbliche parrebbe assicurata esclusivamente mediante un nuovo rilevante carico di prescrizioni, anche laddove vi fossero margini di collaborazione funzionali a garantire l'interesse alla sicurezza cibernetica come interesse nazionale, comune e condiviso dalle istituzioni della Repubblica (per una cybersicurezza cooperativa). Su questo profilo si dirà meglio più avanti, poiché tale approccio emerge con speciale nitidezza dall'impostazione del Capo I, che impone alle pubbliche amministrazioni centrali e del sistema delle autonomie tutta una serie di obblighi di notifica degli incidenti informatici e di risoluzione delle vulnerabilità "potenziali" nei dati e sistemi di loro pertinenza, "tratti" dalla NIS 2, ma declinati in senso fortemente prescrittivo. Non dissimile, sempre sotto il profilo sostanziale, la linea riformatoria del Capo II, improntato al medesimo rigore prescrittivo, espresso anzitutto attraverso l'inasprimento delle pene edittali per i crimini informatici, in un disegno complessivo che peraltro tradisce la rappresentazione di una criminalità informatica 1.0.

Con riguardo al modello regolatorio, come anticipato sopra e specie in relazione al Capo I, una delle maggiori criticità della proposta discende dalla scelta di una fonte ordinaria – apprezzabile "solo" se comparata con la pregressa modalità di regolare la materia per decretazione d'urgenza – che però si muove su piani diversi: in alcuni casi novella le norme previgenti (es. i d.l. convertiti), in altri introduce disposizioni formalmente sganciate dalla regolazione di settore (es. l'art. 10 in tema di appalti). Nessuna misura di coordinamento o previsione di riordino, che auspicabilmente dovrà arrivare col decreto di recepimento della NIS 2. Non è più rinviabile, infatti, una qualche attività manutentiva, un codice (almeno ricognitivo); su tale profilo sembra in parte aprire la delega (art. 3, co. 1, lett. p), legge n. 15/2024: «apportare alla normativa vigente tutte le modificazioni e le integrazioni occorrenti ad assicurare il coordinamento con le disposizioni emanate in attuazione del presente articolo»). Sempre sotto il più generale profilo regolatorio, mancano due clausole essenziali: una prima, col regime transitorio, almeno in relazione ai nuovi oneri e obblighi di cui al Capo I; e una seconda, con la copertura finanziaria. L'intero progetto non è credibile se non si individuano risorse adeguate. In tal senso, in vista della predisposizione della nuova legge di bilancio è opportuno legare le misure del ddl al rifinanziamento dei due fondi sulla cybersicurezza (istituiti con la legge di bilancio per il 2023 – l. 29 dicembre 2022, n. 197, art. 1, co. 899): il "Fondo per l'attuazione della Strategia nazionale di cybersicurezza", per gli investimenti finalizzati all'autonomia tecnologica in ambito digitale e all'innalzamento dei livelli di cybersicurezza dei sistemi informativi nazionali (lett. a); e

il "Fondo per la gestione della cybersicurezza", per finanziare le attività di gestione operativa dei progetti. Infine, si fa particolarmente notare l'assenza di una valutazione d'impatto di alcune delle nuove misure. È pur vero che essa non è prescritta per le proposte in materia di "sicurezza interna ed esterna dello Stato" (che rientra tra i casi di esclusione di cui all'art. 6, co. 1, lett. c), d.P.C.M. 15 settembre 2017, n. 169), ma il Consiglio dei Ministri (o le Commissioni parlamentari poi) avrebbe ben potuto richiederla ai proponenti. Si tratta certamente di una pratica residuale, se non addirittura di un'ipotesi di scuola. Ma certamente una indicazione realistica degli impatti attesi su cittadini, imprese e pubbliche amministrazioni e una effettiva comparazione delle eventuali opzioni regolatorie considerate avrebbero conferito nel merito alla proposta legislativa maggiore qualità. Tenuto conto poi che nel nostro ordinamento nazionale manca una legge annuale sulla transizione digitale, sul modello delle altre leggi periodiche, che potrebbe agevolare il monitoraggio dello stato di attuazione delle norme di settore e la programmazione degli interventi attuativi. In definitiva, quindi, una valutazione pur se minima avrebbe senz'altro rafforzato la "credibilità" dell'intero progetto.

3. Sulla sostenibilità amministrativa (Capo I)

Veniamo ora all'esame più in dettaglio di alcune disposizioni del Capo I, che – come anticipato – potrebbero porre problemi sotto il profilo della sostenibilità amministrativa e più in generale in termini di leale collaborazione tra gli enti interessati dalla nuova normativa. Tra gli altri, destano interesse gli articoli 1 e 2, che estendono alle pubbliche amministrazioni l'ambito di applicazione delle misure di cybersicurezza, di fatto anticipando nel merito il d.lgs. di recepimento della NIS 2. Nello specifico, tali disposizioni introducono obblighi di notifica degli incidenti significativi e di adeguamento alle segnalazioni dell'Agenzia per la cybersicurezza nazionale (ACN), tra gli altri, a carico di regioni e province autonome, comuni con popolazione superiore ai 100.000 abitanti, comuni capoluogo di regione, società di trasporto pubblico con numero di utenti non inferiore a 100.000, aziende sanitarie locali. Tali enti saranno tenuti a notificare gli incidenti informatici che impattano su reti, sistemi e servizi di propria pertinenza, secondo meccanismi di controllo e sanzione (dalla sanzione amministrativa alla responsabilità disciplinare o contabile) gestiti dall'ACN, i cui ulteriori poteri ispettivi non sono precisati, ma verranno declinati con provvedimento del suo direttore. Si ricorda qui che la platea degli incidenti è molto ampia, ricomprendendo tutti gli eventi di natura accidentale o intenzionale che causano malfunzionamento, interruzione (anche parziale) e utilizzo improprio di reti, sistemi informativi o servizi informatici (così l'art. 1, co. 1, lett. h), d.P.C.M. 14 aprile 2021, n. 81). L'art. 2 del ddl disciplina gli obblighi di adeguamento a «segnalazioni puntuali» dell'ACN «circa specifiche vulnerabilità a cui essi risultino potenzialmente esposti», mediante l'adozione al più tardi entro quindici giorni dalla comunicazione delle misure richieste, anche qui con la previsione di oneri informativi e sanzioni per inosservanza. In entrambi i casi, si tratta di misure legislative che possono porre problemi di compatibilità in termini di ordinamento e autonomia organizzativa degli enti ad esse sottoposti, laddove la protezione della sicurezza nazionale rischia di sconfinare nell'autonoma gestione dei sistemi e servizi informativi, veri e propri strumenti di governo delle amministrazioni regionali. Mancando gradualità, tali prescrizioni stridono con l'impostazione cooperativa, verso l'alto e verso il basso, che è determinante per il rafforzamento della cybersicurezza e della resilienza informatica complessiva del sistema Paese. Ciò anche in considerazione del fatto che l'approccio alla sicurezza informatica è un approccio multi rischio, che mira cioè a proteggere dagli incidenti i sistemi informatici e di rete, ma anche il loro ambiente fisico.

Più in particolare, le disposizioni citate chiamano in causa anche aspetti di coordinamento tecnico-informatico, che imporrebbero un approccio condiviso e collaborativo quantomeno con le amministrazioni regionali, nell'ottica di "concorrere" alla definizione del percorso legislativo sulle misure organizzative e strumentali per il rafforzamento della resilienza digitale (per una declinazione della soluzione del "concorso di competenze" in tema di coordinamento orizzontale dei sistemi informativi di amministrazioni statali e regionali, tra le altre, v. Corte cost. n. 50/2005). La questione della base giuridica viene in rilievo proprio in considerazione del carico regolatorio e del meccanismo sanzionatorio previsto dal ddl, che mal

si attaglia alla garanzia della sicurezza nazionale come esigenza anche di unità e indivisibilità di una Repubblica coesa e più (cyber)sicura. Si ricorda al proposito che a partire dal 2005 le regole sulla sicurezza dei sistemi informativi sono state ricondotte agli interventi statali di coordinamento tecnico-informatico che servono a definire le regole tecniche necessarie "per garantire la *sicurezza* (corsivo aggiunto) e l'interoperabilità dei sistemi informatici e dei flussi informativi per la circolazione e lo scambio dei dati e per l'accesso ai servizi erogati in rete dalle amministrazioni medesime" (v. l'art. 14, d.lgs. 7 marzo 2005, n. 82). Come noto, questo coordinamento è oggi affidato a una agenzia della Presidenza del Consiglio, che progetta e monitora l'evoluzione strategica dell'intero sistema informativo pubblico, puntando su infrastrutture e standard comuni o condivisi "che riducano i costi sostenuti dalle amministrazioni e migliorino i servizi erogati" (cfr. *Piano triennale per l'informatica pubblica 2024-2026* cit., p. 10). Con un approccio alla transizione digitale che sin dalle origini considera il sistema informativo pubblico come unitario, strutturato come architettura policentrica e federata, e che oggi risponde peraltro al principio del cloud-first. Un modello in cui stride particolarmente quindi la previsione di interventi verticali posti interamente a carico delle amministrazioni, alle quali non sono destinate risorse specifiche (se si eccettuano quelle "eccezionali" del PNRR già veicolate agli enti mediante gli avvisi dell'ACN). Un vulnus ricorrente in tutte le riforme sulla digitalizzazione pubblica adottate nei decenni passati.

Sotto il profilo della sostenibilità amministrativa, merita attenzione anche l'articolo 6 che disciplina il "rafforzamento della resilienza delle pubbliche amministrazioni". Esso prevede l'istituzione di una nuova "struttura preposta alle attività di cybersicurezza" (co. 1), che potrà essere individuata anche tra quelle esistenti. Al proposito, occorre ricordare che non poche sono le figure che insistono sull'area delle attività connesse al settore digitale: tra queste, il responsabile per la trasparenza, il responsabile per la protezione dei dati personali, il responsabile per la transizione digitale. Quest'ultimo presidia una struttura già normata e dunque l'introduzione di una nuova e autonoma struttura costituirebbe un aggravio organizzativo; sarebbe quindi auspicabile ricondurre ad essa le attività del nuovo referente per la cybersicurezza. Alla nuova struttura sono assegnati compiti sia di indirizzo (v. lett. a): "sviluppo delle politiche"; lett. d): "produzione di un piano programmatico per la sicurezza") sia di carattere tecnico altamente specializzato (v. lett. g): monitoraggio e valutazione continua delle minacce informatiche"). Non sono meglio precisate le competenze del referente per la cybersicurezza, figura peraltro già prevista nell'ultimo "Piano triennale per l'informatica nella PA 2022-2024" adottato dall'Agenzia per l'Italia digitale, a cui quindi la disciplina legislativa nulla aggiunge a proposito dei requisiti professionali. In ogni caso, qualora la competenza fosse altamente specializzata – per ora si può solo intuire – non sarebbe scontato né immediato reclutarla all'interno delle amministrazioni. Al riguardo, oltre al raccordo con le funzioni delle altre strutture menzionate, sarebbe auspicabile la previsione di una fase transitoria e di una "clausola formativa" per programmare un percorso di formazione del personale interno. Frattanto, per far fronte tempestivamente ai numerosi obblighi di legge potrebbe essere consentito il ricorso a figure esterne (come per il Data Privacy Officer) o a un team esterno coordinato da un referente interno all'amministrazione. Una ulteriore soluzione per consentire alle amministrazioni di rispettare le nuove prescrizioni potrebbe essere l'esercizio in forma associata, specie per gli enti di minori dimensioni, o l'affidamento a società in house. Tale ultima ipotesi è stata introdotta di recente anche per lo svolgimento delle attività del referente per la transizione digitale (cfr. l'art. 17, co. 1-*septies*, d.lgs. n. 82/2005), modificato dal d.l. n. 19/2024). Sulle società in house, su cui gravano gli stessi obblighi di notifica e adeguamento previsti dagli artt. 1 e 2, occorrerebbe poi sviluppare nel ddl una disposizione autonoma (un comma aggiuntivo), che precisi la formula opaca "rispettive società in house" inserita in coda all'elenco delle pubbliche amministrazioni obbligate, dettagliando anzitutto i settori merceologici di attività su cui insistono i servizi da esse erogati.

Infine, a proposito di sistema integrato di cybersicurezza, si sottolinea l'assenza di un espresso e chiaro riferimento ai team di risposta agli incidenti di sicurezza informatica (CSIRT) istituiti a livello regionale nell'ambito della struttura nazionale CSIRT Italia (cfr. l'art. 8, d.lgs. 18 maggio 2018, n. 65), che invece potrebbero costituire un raccordo ulteriore con l'istituenda nuova struttura

regionale, ponendosi al contempo come interlocutori degli enti locali: un livello intermedio tra la regione e l'ACN. Tema questo presente nella delega per il recepimento della NIS 2 in cui si prevede di sviluppare e rafforzare la «collaborazione tra tutte le strutture pubbliche con funzioni di Computer Emergency Response Team (CERT) coinvolte in caso di eventi malevoli per la sicurezza informatica» (art. 3, co. 1, lett. e), legge n. 15/2024). Resta poi sullo sfondo la natura giuridica del CSIRT regionale, per chiarire il rapporto con gli enti regionali (le misure organizzative e le risorse) e standardizzare il procedimento costitutivo.

Per concludere su questi profili, una struttura così complessa avrebbe imposto anzitutto una valutazione della sostenibilità amministrativa, che manca nella documentazione a corredo dell'atto, ma – come detto sopra – avrebbe giovato alla definizione di misure per molta parte "rimesse" quindi nel breve periodo alla capacità o incapacità dei singoli enti.

4. Nota finale sulla governance

Dal quadro sopra appena tratteggiato, e da altre disposizioni del ddl qui non approfondite, pare delinearsi anche una rinnovata governance della cybersicurezza, sempre più imperniata sulle (sole) agenzie governative della Presidenza del Consiglio. L'ACN acquisterebbe poteri in materia di cybersicurezza più penetranti di natura accertativa e sanzionatoria, ma anche nuove funzioni in relazione per esempio allo sviluppo delle applicazioni di intelligenza artificiale (IA) quale "risorsa per rafforzare la cybersicurezza" (art. 7, co. 1). Un innesto che trova ampio seguito anche nel draft del ddl governativo sull'intelligenza artificiale (approvato dal Consiglio dei Ministri il 23 aprile 2024) nel quale la cybersicurezza è indicata come "precondizione essenziale" dell'IA e l'ACN si troverebbe a condividere con l'Agenzia per l'Italia digitale il ruolo di Autorità nazionale per l'intelligenza artificiale (art. 18). Anche le attività di coordinamento e raccordo con le amministrazioni pubbliche e le autorità indipendenti, pure previste (al comma 2 dell'art. 18), sono appannaggio della Presidenza del Consiglio presso cui si prevede di costituire un apposito Comitato di coordinamento, che sarà appunto interno alla Presidenza e si comporrà dei direttori delle due Agenzie e del Capo del Dipartimento PCM per la trasformazione digitale. Questa linea parrebbe confermare quell'approccio accentratore e verticalizzante di cui si è detto al principio a proposito del ddl 1717. Resta fermo che per meglio valutare gli esiti di entrambe le proposte legislative occorrerà attendere che si concluda l'esame parlamentare appena avviato.

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0147 • articolo sottoposto a peer review • pubblicato in anteprima il 17 mag. 2024

Pier Giorgio Chiara

DDL Cybersicurezza: tra l'inasprimento della risposta penale del legislatore nazionale e il modello preventivo-amministrativo della direttiva NIS2

L'Autore è assegnista di ricerca in informatica giuridica dell'Università di Bologna, CIRSFID ALMA-AI

La ricerca è stata svolta nell'ambito del Progetto PNRR "Partenariato Esteso" *SERICS - SEcurity and RIghts in the CyberSpace*, *Spoke 8 - Ecocyber* (CUP J33C22002810001), finanziato dall'Unione europea - Next Generation EU

Questo contributo fa parte della sezione monografica *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2* – Instant Book, a cura di Gaia Fiorinelli e Matteo Giannelli

I. Il disegno di legge recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici, c.d. DDL Cybersicurezza (da qui in avanti, 'DDL'), presentato il 16 febbraio 2024, consta di due capi, che individuano le due anime principali di questo provvedimento legislativo. Se il capo I individua norme di "cyber resilienza", volte ad elevare, cioè, la capacità di protezione e risposta di fronte a minacce cibernetiche in costante evoluzione, crescita e sofisticatezza, nonché di governance della cybersicurezza nazionale, il capo II inasprisce la risposta penale attraverso disposizioni di natura sostanziale e processuale mirate al contrasto dei reati informatici.

Senza entrare ora nel dettaglio delle singole disposizioni, è opportuno sottolineare in via preliminare come il DDL non operi in un *vacuum* normativo bensì si raccordi – e modifichi – la c.d. "normativa PSNC", ovvero il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133 (unitamente ai diversi regolamenti attuativi) e il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.

In particolare, si estende ai soggetti rientranti nella normativa PSNC l'obbligo di provvedere entro quindici giorni dalla comunicazione dell'Agenzia per la Cybersicurezza Nazionale (ACN) circa specifiche vulnerabilità cui essi risultino potenzialmente esposti mediante interventi risolutivi indicati dall'Agenzia (art. 2 DDL). Sulla scorta del modello NIS 2 in materia di notifica degli incidenti, i soggetti PSNC dovranno effettuare una segnalazione entro 24 ore dall'avvenuta conoscenza di incidenti aventi impatto su reti, sistemi informativi e servizi informatici di propria pertinenza diversi da quelli 'perimetrati', da completarsi con la relativa notifica entro il termine di 72 ore. Inoltre, qualora i soggetti reiterino l'inosservanza di questa previsione, saranno passibili di una sanzione amministrativa pecuniaria fino ad un massimo di 125.000 euro (art. 3 DDL). Viene poi specificata una modalità di funzionamento del Nucleo per la cybersicurezza (art. 5 DDL); è prevista, come

nuova funzione di ACN, la produzione e diffusione di standard e raccomandazioni in materia di crittografia al fine di rafforzare la cybersicurezza dei sistemi informatici (art. 10 DDL) e, infine, si è prevista l'adozione di un regolamento per la disciplina del procedimento sanzionatorio amministrativo di ACN (art. 11 DDL).

Il presente contributo mira a far luce su un aspetto critico sollevato dal DDL, vale a dire, la risposta del legislatore nazionale in materia di cybersicurezza imperniata *principalmente* sull'aumento ed inasprimento della repressione penale alla luce di un modello, quello della Direttiva (UE) 2022/2555 (c.d. direttiva NIS 2), che, di converso, prevede *inter alia* un complesso quadro di strumenti di prevenzione e gestione del rischio di cybersicurezza di stampo più marcatamente privatistico-amministrativistico. Se è pacifico che la risposta penale sia una prerogativa degli Stati membri, la premessa da cui parte questo elaborato – e che si cercherà di avvalorare – è che il modello anticipatorio delineato dalla normativa NIS 2 sia più efficace di un modello repressivo-deterrente nell'affrontare le sfide poste dalla cybersicurezza, del tutto peculiari rispetto a quelle con cui i sistemi giuridici si confrontano nella dimensione analogica.

In questo contesto, una lettura che è possibile avanzare è che tale 'salto in avanti' del legislatore italiano, nelle more del recepimento della direttiva NIS 2, sia legato ad un più generale problema che caratterizza la regolamentazione della cybersicurezza nell'Unione: la tendenza a declinare questa in termini di sicurezza nazionale o di funzionamento del mercato interno e di cooperazione, a seconda del fatto che l'iniziativa legislativa venga presa rispettivamente dagli Stati membri o dalla Commissione europea.

II. Mentre il panorama delle minacce cibernetiche cresce in estensione e complessità, il legislatore nazionale dedica metà del nuovo provvedimento in materia al rafforzamento delle misure di contrasto di alcuni reati informatici. Si potrebbe obiettare che le disposizioni di cui al primo capo del DDL mirino proprio al rafforzamento di un modello di cyber resilienza simile a quello comunitario, con particolare riferimento alla direttiva NIS 2.

A tal proposito, si pensi all'art. 8, che impone alle pubbliche amministrazioni rientranti nell'ambito del DDL di individuare una struttura (all'interno della quale opererà il c.d. referente per la cybersicurezza quale punto di contatto unico dell'ente) che provvederà allo sviluppo di politiche e procedure di sicurezza delle informazioni (es., definizioni di ruoli e organizzazione del sistema), alla produzione e all'aggiornamento di un piano per la gestione del rischio cyber, nonché alla pianificazione e attuazione di interventi di potenziamento delle capacità di gestione del rischio e dell'adozione delle misure previste dalle linee guida da emanare con determina del direttore di ACN. Oppure, sotto diverso profilo, si pensi all'allineamento dei termini per gli obblighi di notifica di cui all'articolo 1, comma 2, DDL ai termini di cui all'articolo 23 della direttiva NIS 2.

Eppure, per quanto l'articolo 2, comma 5, della direttiva NIS 2 riconosca piena autonomia agli Stati membri nel decidere se la direttiva si applichi alle PA a livello locale (gli enti della PA a livello centrale sono infatti soggetti essenziali NIS 2, ex art. 3, comma 1, lett. d), è legittimo chiedersi perché 'anticipare' in questo provvedimento quanto avrebbe potuto essere disposto nel decreto legislativo di recepimento della NIS 2 (da adottare entro ottobre 2024). Ancorché sia imperativo per il nostro legislatore trovare nel futuro atto di attuazione della norma comunitaria un necessario raccordo con le disposizioni qui menzionate – al fine di evitare duplicazioni degli obblighi per tali soggetti – una scelta di diversa politica legislativa avrebbe portato con sé il beneficio di non frammentare ulteriormente un quadro normativo nazionale che, per quanto recente, risulta essere un "mosaico" di già diversi decreti-legge e decreti legislativi, DPR, DPCM, nonché determine del Direttore di ACN.

Veniamo ora al tema dell'efficacia della deterrenza sanzionatoria di stampo penalistico nell'ambito della cybersicurezza. Il tradizionale modello penalistico, in questo contesto, deve fronteggiare due sfide principali, tra loro correlate: la progressiva marginalità e debolezza della sovranità nazionale e la necessità di una risposta efficace alle minacce ed ai reati informatici. I rischi, le minacce e gli attacchi nel cyberspazio non sono più appannaggio esclusivo di attori statali, che devono riconoscere il potere *de facto* esercitato da attori privati. È opportuno ricordare come già la prima strategia UE in materia di cybersicurezza nel 2013 identificasse in un approccio multi-stakeholder la chiave per una gestione efficace delle sfide della dimensione digitale. Inoltre, la cybersicurezza è

intrinsecamente transnazionale. Ad incidere pertanto negativamente sulla tradizionale risposta penalistica vi sono, in primo luogo, le difficoltà nell'identificare e localizzare criminali informatici – spesso sufficientemente schermati da tecniche di anonimato – che operano in giurisdizioni diverse. Qualora si riuscisse poi ad identificare e perseguire il criminale, vi sarebbero poi delle sfide legate all'estradizione. Un altro elemento di complessità è dato dalla scarsa disponibilità di dati relativi alla criminalità informatica, anche alla luce della bassa percentuale di reati segnalati, ecc.

Peraltro, rimanendo sul piano della risposta penalistica, il DDL potrebbe essere letto come un'occasione mancata per l'introduzione di regole *ad hoc* di natura sostanziale e processuale, per esempio con riferimento all'espletamento di pagamenti da parte delle aziende a seguito di c.d. attacchi *ransomware*, *ethical hacking* o ancora in materia di competenza territoriale dei pubblici ministeri in tema di reati informatici.

Invece, come già ricordato, la direttiva NIS 2 sposta l'attenzione della risposta ai rischi, alle minacce e agli incidenti "a monte", attraverso un modello di governance articolato soprattutto intorno alla dimensione preventiva. Infatti, la direttiva NIS 2 declina il c.d. "approccio al rischio" – che permea la quasi totalità degli atti giuridici UE sul digitale – attraverso un complesso reticolato di quadri coordinati di cooperazione a livello nazionale, comunitario (es., Gruppo di cooperazione NIS; rete di CSIRTs; EU-CyCLONe), e internazionale (accordi internazionali *ex* art. 17 NIS 2); tramite l'incoraggiamento della condivisione di informazioni pertinenti (es., minacce, indicatori di compromissione, tecniche e procedure, ecc.) tra soggetti NIS e delle pratiche di divulgazioni coordinate delle vulnerabilità (attraverso l'istituzione di una banca dati europea delle vulnerabilità mitigate) al fine di aumentare il livello collettivo di cybersicurezza prevenendo così incidenti. Sempre sul fronte della prevenzione, la direttiva NIS 2 delinea poi un quadro di misure tecniche, operative e organizzative di valutazione e gestione dei rischi da parte dei soggetti NIS 2: il c.d. "approccio al rischio" si sostanzia nella responsabilizzazione del soggetto NIS, il quale dovrà adottare misure adeguate e proporzionate al rischio posto alla sicurezza dei suoi sistemi, secondo un approccio multi-rischio (protezione dell'ambiente fisico ed informatico).

Il DDL dovrebbe quindi porre maggiormente l'accento su questi aspetti 'anticipatori' e prevedere, quantomeno, dei regolamenti attuativi in cui vengano definite delle linee guida affinché le pubbliche amministrazioni interessate dal DDL riescano a conformarsi agli obblighi di cui all'art. 8 DDL, permettendo pertanto un rafforzamento effettivo – e non solo "sulla carta" – della cybersicurezza di tali soggetti, anche considerata la clausola di invarianza finanziaria di cui all'art. 23 DDL.

III. L'accento posto dal legislatore italiano sulla risposta repressiva all'accrescere delle minacce e degli attacchi cibernetici può essere letto con la lente dei conflitti di competenza, spesso silenziosi, tra l'UE e gli Stati membri nel regolamentare le questioni legate alla cybersicurezza. La vaghezza delle definizioni e dei concetti cardinali delle politiche di cybersicurezza all'interno dell'Unione è elemento imprescindibile di questa teoria. Infatti, sembra che i perimetri concettuali, nonché gli obiettivi perseguiti dal termine stesso di "cybersicurezza" (oppure ancora, "resilienza") varino a seconda di chi legiferi.

Gli Stati membri tendono a dotarsi di normative in materia di cybersicurezza facendo perno su aspetti di sicurezza nazionale (es., Italia, Estonia, Germania), la quale è competenza nazionale esclusiva di ciascuno Stato membro ex art. 4, paragrafo 2 del Trattato sull'Unione europea. In tal senso, non può stupire che tale riferimento normativo sia richiamato esplicitamente dall'analisi tecnico-normativa del DDL Cyber (A.C. 1717 Supplemento, p. 17). Nel caso italiano, una lettura congiunta del titolo della normativa di cui al decreto-legge n. 105 del 2019 e dell'articolo 1 del medesimo decreto suggerisce la volontà del legislatore di governare un'area specifica della sicurezza nazionale.

A un più basso livello di astrazione, tuttavia, le disposizioni della normativa PSNC si sovrappongono in larga misura – se non addirittura duplicano – con il quadro giuridico della NIS 2. Infatti, la Commissione europea disegna una governance europea della cybersicurezza partendo però da logiche diverse, ossia, di funzionamento del mercato interno e di cooperazione.

Dall'inizio degli anni 2000 possono essere rintracciati diversi "scontri" sulle competenze tra l'UE e gli Stati membri in materia di cybersicurezza: dall'istituzione dell'ENISA nel 2004, che si è vista progressivamente affidare compiti

tradizionalmente di appannaggio degli stati; alle posizioni divergenti tra Consiglio dell'UE, da una parte, e Parlamento e Commissione dall'altra, con il primo pronto a rimarcare la competenza statuale ex art. 4, paragrafo 2 TUE anche in materia di cybersicurezza in dossier legislativi come il *Cyber Resilience Act* (si vedano le posizioni circa una governance centralizzata/decentralizzata degli obblighi di notifica), *Cyber Solidarity Act* (che istituisce meccanismi di coordinamento a livello sovranazionale di gestione delle crisi e incidenti di cybersicurezza su larga scala, terreno che facilmente gli stati riconducono ai perimetri di sicurezza nazionale) o ancora la proposta del 2020 di una *Joint Cyber Unit* (poi mai concretizzatasi).

Connesso a ciò, rimane il difficile compito di tracciare i confini tra "cybersicurezza" e "sicurezza nazionale". Gli stessi eventi avversi descritti come minacce informatiche potrebbero al tempo stesso essere definiti come reati, ossia questione interna per eccellenza. Atteso che il confine tra minaccia cibernetica e crimine cibernetico sia tutt'altro che chiaro, il quadro giuridico sotteso alle competenze e strumenti cambia radicalmente. Se consideriamo la cybersicurezza come una questione di mercato unico digitale (vedi NIS 2, *Cybersecurity Act*, *Cyber Resilience Act*), o di competitività del sistema industriale dell'Unione (*Cyber Solidarity Act*), l'Unione ha competenza per disporre misure regolamentative non solo su standard tecnici comuni, ma anche su meccanismi comuni di indagine e reazione. Se consideriamo la lotta contro le minacce informatiche come una questione di diritto penale, come si è fatto per molto tempo (es., Convenzione di Budapest), tuttavia, il panorama è non solo diverso, ma anche meno efficace rispetto al modello comunitario, come visto sopra.

Senza entrare nel merito di quale ruolo possa (ancora) svolgere *efficacemente* il sistema giudiziario penale in questo contesto, come suggerito da Enrico Letta nel suo report *Much More than a Market* (aprile 2024), dietro incarico della dalla Commissione e dal Consiglio UE, l'imposizione di requisiti aggiuntivi da parte dei legislatori nazionali motivati da logiche connesse alla sicurezza nazionale, come nel caso italiano, rischia di erodere i benefici del mercato unico aumentando i costi e creando incertezza per le imprese. Per affrontare questo problema, è indispensabile garantire che questi requisiti siano in linea con il quadro legislativo europeo generale, adottando misure aggiuntive solo se assolutamente necessarie (p. 59).

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0143 • articolo sottoposto a peer review • pubblicato in anteprima il 17 mag. 2024

GAIA FIORINELLI

Il *ransomware* nel DDL Cybersicurezza: dalla fattispecie di estorsione "informatica" al coordinamento tra indagini e *incident response*

L'Autrice è ricercatrice in Diritto penale alla Scuola Superiore Sant'Anna di Pisa

La ricerca è stata svolta nell'ambito del Progetto PNRR "Partenariato Esteso" *SERICS - SEcurity and RIghts in the CyberSpace, Spoke 1 – Cyberights* (CUP J53C22003110001), finanziato dall'Unione europea - Next Generation EU

Questo contributo fa parte della sezione monografica *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2* – Instant Book, a cura di Gaia Fiorinelli e Matteo Giannelli

1. Tra gli interventi di maggiore interesse previsti dal Capo II del ddl Cybersicurezza si segnala la proposta di introdurre un'apposita fattispecie penale denominata «estorsione informatica» o «estorsione mediante reati informatici» (art. 15, co. 1, lett. m), mediante la quale s'intende reagire alla «gravità» e alla «frequenza» dei «ricatti realizzati attraverso la minaccia o l'attuazione di attacchi informatici» (ddl, p. 7).

Il ddl fa riferimento ai c.d. attacchi *ransomware*, che, secondo i dati del C.N.A.I.P.I.C., hanno costituito nel 2023 la tipologia più diffusa di "attacchi gravi" (34%), con un rilevante impatto a livello nazionale sulla PA e sull'erogazione di servizi (Clusit 2024). Come rilevato da ENISA e dal *Cybercrime Convention Committee* del Consiglio d'Europa, gli attacchi *ransomware* rappresentano una delle forme più gravi di cybercriminalità dell'ultimo decennio, ai danni di individui, imprese e pubbliche amministrazioni (ENISA 2022; T-CY 2022); nondimeno, si tratta di una fenomenologia criminosa che, in virtù della particolare complessità dell'*iter criminis*, risulta tuttora priva di una rilevanza penale unitaria, potendo un singolo attacco *ransomware* integrare molteplici (ma distinti) reati (informatici e non) nelle singole fasi della sua esecuzione (Cybercrime Convention Committee 2022), con un connesso rischio di parcellizzazione e dispersione delle attività di *law enforcement* (Wall 2021).

Prima di analizzare la soluzione ideata dal legislatore italiano, occorre rilevare come un attacco *ransomware* (dall'inglese *ransom*, «riscatto») si componga generalmente (e semplificando): (i) di una prima fase più propriamente "informatica", nella quale l'attaccante introduce in vario modo un *malware* nel computer *target*, per criptare file, altri contenuti o il sistema stesso e renderli così inaccessibili al titolare (più nel dettaglio: ENISA, 2022); e (ii) di una seconda fase invece "estorsiva", nella quale l'attaccante richiede al bersaglio il pagamento di un riscatto (solitamente in criptovalute), in cambio del ripristino della funzionalità o dell'accessibilità dei dati o del sistema (Cybercrime Convention

Committee 2022), ovvero (o anche) dietro la minaccia di segnalare il *data breach* alle autorità o di divulgare pubblicamente i dati o la loro violazione, o ancora di venderli sul *dark web* (c.d. doppia estorsione; Hyslip-Burruss 2023; ENISA 2022). Come rilevato da Europol (Europol 2023), inoltre, dietro gli attacchi *ransomware* si celano spesso gruppi strutturati secondo il *business model* del *crime-as-a-service* (o *ransomware-as-a-service*), incentrati su "programmi di affiliazione" aperti alla libera adesione da parte di utenti della rete, i quali possono contribuire dietro compenso a una delle molteplici fasi del "processo", secondo il paradigma definito dalla letteratura criminologica «crimine *(dis)organizzato*» (Wall 2015).

Per reagire a questa fenomenologia criminosa, fonte di un crescente allarme sociale – anche in quanto realizzata, sempre più spesso, ai danni di pubbliche amministrazioni –, il legislatore si propone d'intervenire sia sul piano del diritto penale *sostanziale*, sia mediante un migliore coordinamento *procedurale* tra le attività di indagine e le attività di c.d. *incident response*, sul presupposto che, nel caso di attacchi informatici, il perseguimento prioritario di un'esigenza (indagine, oppure ripristino tempestivo) rischi spesso di compromettere l'altra.

2. L'art. 15, co. 1, lett. m del ddl prevede, dunque, l'introduzione di un terzo comma nell'art. 629 c.p. (*Estorsione*), per punire chiunque «costring[a] taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno», mediante le «condotte di cui agli articoli 615-*ter*, 617-*quater*, 617-*sexies*, 635-*bis*, 635-*quater* e 635-*quinquies*» ovvero la «minaccia di compierle». In buona sostanza, nella "estorsione informatica" la *violenza* e la *minaccia*, che costituiscono le condotte tipiche produttive della costrizione nella fattispecie di estorsione "comune" (Marini 1990), sono sostituite dal riferimento alle *condotte* di una serie di reati informatici (*Accesso abusivo, Intercettazione, impedimento, etc. […] o Falsificazione, alterazione, etc. […] di comunicazioni informatiche, Danneggiamento di informazioni, dati e programmi informatici, Danneggiamento di sistemi informatici,* anche *di pubblica utilità),* ovvero alla «*minaccia di compierle*».

In termini generali, si può accogliere con favore l'intento del legislatore di "aggiornare" le fattispecie penali relative al *cybercrime*, a fronte di fenomeni criminosi, come il *ransomware*, che si sono diffusi in epoca recente e che solo con difficoltà possono ricondursi alle incriminazioni già esistenti. Invero, sebbene non manchino disposizioni per qualificare penalmente i singoli segmenti del complessivo *iter criminis* (dalla programmazione del *malware*, al danneggiamento del sistema informatico, etc.: Cybercrime Convention Committee 2022), nessuno dei "reati informatici" esistenti intercetta il disvalore della componente "estorsiva" degli attacchi *ransomware* e la loro conseguente natura pluri-offensiva (che unisce alla violazione della sicurezza informatica l'eventuale lesione patrimoniale e la lesione della libertà di autodeterminazione della vittima).

Del resto, anche l'applicazione della fattispecie di estorsione "comune" a questa tipologia di attacchi solleva alcune questioni interpretative. Nonostante, ad esempio, l'Agenzia delle Entrate, nella risposta n. 149/2023, si sia espressa per la generale riconducibilità dei casi di *ransomware* all'art. 629 c.p., non risulta affatto scontata la possibilità di qualificare le condotte di "aggressione informatica" realizzate dai *cyber*-attaccanti, pur potenzialmente produttive di una *costrizione*, alla stregua delle nozioni di *violenza* o *minaccia* di cui all'art. 629, co. 1, c.p. Con riguardo alla *violenza*, potrebbe invero farsi riferimento all'art. 392, co. 3, c.p., che configura la *violenza sulle cose* anche allorché sia danneggiato un programma informatico o sia turbato il funzionamento di un sistema informatico (senza nessun riferimento, tuttavia, al "sequestro" dei dati). Con riferimento alla *minaccia*, invece, nella maggior parte degli attacchi, più che la prospettazione di un male ingiusto, si riscontra una "aggressione informatica" già compiuta, antecedente rispetto alla richiesta di "riscatto" (sul punto, tuttavia, la giurisprudenza riconduce alla nozione di *minaccia estorsiva* anche la richiesta di denaro accompagnata dalla prospettazione della mancata restituzione del bene sottratto: Cass. pen., sez. II, n. 25213/2019).

3. Poste tali premesse di ordine generale, s'intende anche sottolineare come la fattispecie descritta nel disegno di legge presti il fianco ad alcune censure.

In primo luogo, la realtà degli attacchi *ransomware* avrebbe reso forse preferibile, in luogo del ricorso *tout court* alla fattispecie di estorsione, il "recupero" del modello del "reato commesso *a scopo di estorsione*" (il quale già nel codice Zanardelli era punito a titolo di "ricatto", quale fattispecie

distinta dall'estorsione, e che tuttora, secondo giurisprudenza costante, presenta una struttura diversa rispetto all'art. 629 c.p., come affermato ad es. da Cass. pen., Sez. Unite, n. 962/2003). Tale diversa struttura della fattispecie parrebbe preferibile non foss'altro perché, ad esempio, nel caso del delitto commesso *a scopo di estorsione* il reato sarebbe integrato a prescindere dall'avvenuto versamento del "prezzo della liberazione" dei sistemi informatici o dei dati (posto che il profitto costituirebbe soltanto l'oggetto del dolo specifico), mentre nell'estorsione il conseguimento del profitto ingiusto rappresenta un elemento costitutivo del reato, in assenza del quale può ritenersi tutt'al più integrata la fattispecie tentata (per un esempio dell'uso del requisito dell'*intent to extort* per la costruzione del reato di "*ransomware*" nel § 523 *California Penal Code*: Lubin 2022).

Anche in una prospettiva sistematica, peraltro, non va trascurato come in casi analoghi (es. sequestri di persona), alla riforma del delitto di estorsione (mediante una specificazione dei mezzi con funzione aggravante), sia stata preferita la creazione di varianti "a dolo specifico" (punite più gravemente) di fattispecie a "fine generico", per realizzare una «specializzazione della tutela» (Padovani 2023) funzionale a enucleare il diverso «significato offensivo» del perseguimento di una specifica e ulteriore *finalità* (ad es. estorsiva), nella commissione di un determinato reato (es. sequestro di persona).

Tale questione strutturale si riverbera, del resto, sulla stessa definizione del trattamento sanzionatorio. Per la fattispecie di "estorsione informatica", infatti, l'art. 15, co. 1, lett. m del ddl prevede limiti edittali molto elevati (reclusione da sei a dodici anni e multa da euro 5.000 a euro 10.000 per la fattispecie "base") e, soprattutto, più elevati rispetto a quelli dell'estorsione "comune" di cui al co. 1. Se, tuttavia, la finalità offensiva *ulteriore* generalmente giustifica la comminatoria di pene più elevate nei delitti a dolo specifico (rispetto alle ipotesi a "fine generico"), non è invece scontato che il ricorso a un "mezzo informatico" sia in ogni caso più grave, rispetto alla *violenza* o alla *minaccia*, nella commissione del delitto di estorsione. Il nuovo co. 3 dell'art. 629 c.p., dunque, parrebbe creare una disparità di trattamento potenzialmente irragionevole (in termini suscettibili di censura d'illegittimità costituzionale; Frigo 2013). Può dubitarsi, infatti, che l'estorsione *informatica* sia di per sé e in ogni caso *più grave* rispetto all'estorsione "comune", nella quale la violenza o la minaccia possono attingere anche l'integrità fisica della persona offesa; soprattutto, la potenziale irragionevolezza emerge nei casi virtualmente già rientranti nell'art. 629, co. 1, c.p. (ad es., la «*minaccia di compier[e]*» reati informatici, prevista dal nuovo co. 3, sarebbe già rilevante alla stregua di ordinaria *minaccia* ai sensi del co. 1, ma risulterebbe tuttavia punita più gravemente di ogni altra minaccia estorsiva).

Venendo, poi, alle ipotesi aggravate – punite con la pena (anch'essa molto elevata) della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000 – la riforma si espone a una censura in punto di tecnica legislativa. Per l'individuazione delle aggravanti, infatti, la disposizione rinvia alle "circostanze indicate nell'ultimo capoverso" dell'art. 628 c.p., riprendendo la stessa formulazione dell'art. 629, co. 2, c.p.: tale disposizione, tuttavia, già scontava un difetto di coordinamento con lo stesso art. 628 c.p., a seguito dell'introduzione, in tale ultima disposizione, di due ulteriori commi (dopo il co. 3 che elenca le aggravanti) nel 2009 e nel 2017. Se, dunque, già l'art. 629, co. 2, c.p. necessiterebbe di aggiornamento, è criticabile che la disposizione di nuova introduzione ne riproduca persino il mancato coordinamento con le modifiche dell'art. 628 c.p. (correttamente la proposta emendativa 11.24 tentava di ovviare a tale inconveniente, ma non è stata approvata). Del resto, la disciplina risultante dal rinvio si appalesa doppiamente insoddisfacente. Per un verso, infatti, si rinvia "in blocco" alle aggravanti previste per il delitto di rapina, senza considerare che la maggior parte di esse risulterà assolutamente inapplicabile agli attacchi *ransomware*, in virtù della differente dinamica esecutiva (ad es. la commissione con uso di armi, o da parte di persona travisata, o in luoghi di privata dimora, o di pubblico trasporto, o nei confronti di persona che si trovi nell'atto di fruire dei servizi di istituti di credito, uffici postali o sportelli automatici, per citarne soltanto alcune). Per altro verso, la disposizione risulta disallineata rispetto alle aggravanti speciali previste per gli altri reati informatici, anche sulla base del medesimo ddl (si fa riferimento all'elenco di aggravanti tipizzate dall'art. 615-*ter*, co. 2 e 3, c.p., ove ad es. si sottopone a pena più elevata l'attacco realizzato ai danni di un sistema informatico di interesse pubblico, alle quali, all'esito del riordino proposto

nel ddl, rinvierebbero gli artt. 615-*quater*, 617-*bis*, 617-*quater*, 635-*quater*.1 c.p.).

4. Completano la disciplina penale della nuova «estorsione informatica» alcune ulteriori disposizioni "di contorno".

Anzitutto, risulteranno applicabili anche ai casi previsti dall'art. 629, co. 3, c.p. le nuove circostanze attenuanti del "fatto di lieve entità" (attenuante a effetto comune) e del "ravvedimento"/"collaborazione" *post delictum* (attenuante a effetto speciale), previste dal nuovo art. 639-*ter* c.p. (art. 15, co. 1, lett. s). La disposizione riproduce un modello frequentemente adottato dal legislatore, specie in abbinamento con un generale inasprimento delle pene (secondo un approccio "*stick and carrot*" esplicitato nella stessa relazione al ddl): se il riferimento alla «lieve entità» risulta coerente (almeno rispetto alla fattispecie di estorsione) con la sentenza della Corte costituzionale n. 120/2023, e postulerà una valutazione di natura, specie, mezzi, modalità o circostanze dell'azione, nonché del danno o pericolo, la riduzione di pena per la collaborazione *post delictum* corrisponde a un modello concepito inizialmente per i reati di criminalità organizzata e progressivamente esteso dal legislatore a diversi settori di criminalità "plurisoggettiva" (tuttavia, a differenza di quanto si prevede, ad es., in materia di reati contro la PA, non si richiede in questo caso che la collaborazione sia *efficace*).

Piuttosto inconferente con la realtà criminologica degli attacchi *ransomware* può risultare invece la previsione dell'art. 19 del ddl, nella parte in cui modifica l'art. 24-*bis* del d.lgs. 8 giugno 2001, n. 231, inserendo l'art. 629, co. 3, c.p. tra i reati presupposto della responsabilità amministrativa da reato dell'ente: come si anticipava, risulta difficile ipotizzare che gli attacchi *ransomware* possano promanare dagli enti economici che costituiscono i principali destinatari del d.lgs. 231/2001, trattandosi nella maggior parte di attività riconducibili a veri e propri gruppi criminali.

Sempre con riferimento alla disciplina collaterale, si segnala ancora l'omesso rinvio all'art. 629, co. 3, c.p. nelle disposizioni processuali modificate dall'art. 16 (che non estende all'estorsione informatica né la specifica competenza della Procura distrettuale, né il regime derogatorio in tema di durata delle indagini preliminari e proroga dei termini), con una conseguente asimmetria che, almeno a prima lettura, risulta ingiustificata.

5. Ancora, si vuole segnalare come, proprio per la gestione di attacchi di questo tipo – specialmente se realizzati ai danni di sistemi di pubblico interesse (in commissione il Sottosegretario Mantovano ha richiamato, quale caso paradigmatico, il «blocco della sala operatoria», rispetto al quale ci si domanda se sia «meglio ripristinarla subito», anche a costo di «altera[re] la scena del crimine», oppure se debbano privilegiarsi le esigenze di indagine, a costo di «lascia[re] bloccata la sala operatoria») –, il ddl Cybersicurezza disciplini anche, all'art. 21, il coordinamento tra attività d'indagine e *incident response*. In tale direzione, oltre ai reciproci obblighi di informazione tra il Procuratore Nazionale Antimafia e antiterrorismo e ACN, in relazione ai casi di comune competenza (es. art. 371-*bis*, co. 4-*bis*, c.p.p. e altri elencati), il nuovo co. 4-bis.3 dell'art. 17 d.l. 14 giugno 2021, n. 82 (conv. l. 109/2021), per come riformulato dall'art. 21, co. 1, lett. b del ddl non soltanto prevede che spetti al Pubblico Ministero impartire le disposizioni necessarie, in fase di indagine, per assicurare che gli accertamenti urgenti siano compiuti tenendo conto delle attività svolte dall'ACN ai fini di resilienza, ma soprattutto gli attribuisce la facoltà di disporre il differimento (motivato) di una di tali attività, qualora ciò sia necessario per evitare un grave pregiudizio per il corso delle indagini. Nel testo del ddl è, dunque esplicita la "poziorità" delle attività investigative sulle operazioni di *cyber*-resilienza, contenimento e ripristino: se la scelta è coerente con l'impostazione marcatamente "punitiva" del provvedimento, nel contesto internazionale la soluzione è invece la progressiva integrazione operativa tra *digital forensics* e *incident management* (Kent et al. 2006).

6. In conclusione, deve rilevarsi come l'intervento legislativo proposto con il ddl, nonostante l'apparente (quanto simbolica) "severità" nel ricorso allo strumento punitivo, risulti destinato a una scarsa efficacia quanto al contrasto degli attacchi *ransomware*. Invero, il ddl si limita all'introduzione della fattispecie di "estorsione informatica" senza contestualmente affrontare i principali nodi critici che tuttora ostacolano il perseguimento dei c.d. *computer crime* (ad es. la difficile identificazione degli autori e attribuzione degli attacchi; la proiezione extra-territoriale della giurisdizione nazionale), non valorizza la realtà empirico-criminologica dei *ransomware* (nella misura in cui, ad es., non

attribuisce rilevanza alle dinamiche di affiliazione in programmi di *crime-as-a-service*; non prevede alcuno strumento *patrimoniale*, sebbene si tratti di attacchi imperniati sulla richiesta di un "riscatto"; non disciplina il pagamento del *ransom*, nemmeno con un obbligo di notifica; non interviene sul "mercato nero" dei dati (Hyslip-Burruss 2023), né valorizza possibili strumenti innovativi (ad es. *blockchain analytics*, per tracciare le transazioni in *bitcoin*).

Riferimenti bibliografici

Clusit (2024), *Rapporto 2024 sulla sicurezza ICT in Italia*, 2024

Cybercrime Convention Committee (2022), *T-CY Guidance Note #12. Aspects of ransomware covered by the Budapest Convention*, 2022

ENISA (2022), *Threat Landscape for Ransomware Attacks*, 2022

Europol (2023), *Cyber-attacks: the apex of crime-as-a-service*, 2023

G. Frigo (2013), *I principi di proporzionalità e ragionevolezza nella giurisprudenza costituzionale italiana in materia penale*, 2013

T.S. Hyslip, G.W. Burruss (2023), *Ransomware*, in D. Hummer, J. Byrne (eds.), "Handbook on Crime and Technology", Edward Elgar Publishing, 2023

K. Kent, S. Chavalier, T. Grance, H. Dang (2006), *Guide to Integrating Forensic Techniques into Incident Response*, 2006

A. Lubin (2022), *The Law and Politics of Ransomware*, in "Vanderbilt Journal of Transnational Law", vol. 55, 2022

G. Marini (1990), voce *Estorsione*, in "Digesto delle Discipline Penalistiche", Utet, vol. IV, p. 377 ss., 1990

T. Padovani (2023), *Diritto penale,* XII ed., Giuffrè, 2023

D.S. Wall (2021), *The Transnational Cybercrime Extortion Landscape and the Pandemic: Changes in Ransomware Offender Tactics, Attack Scalability and the Organisation of Offending*, in "European Law Enforcement Research Bulletin", 2021

D.S. Wall (2015), *Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime*, in "The European Review of Organised Crime", vol. 2, 2015, n. 2

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0148 • articolo sottoposto a peer review • pubblicato in anteprima il 17 mag. 2024

Gaetana Morgante

L'estensione dello statuto penale della criminalità organizzata di stampo mafioso alla cybercriminalità diretta contro sistemi informatici e telematici "pubblici"

L'Autrice è professoressa ordinaria di Diritto penale alla Scuola Superiore Sant'Anna di Pisa

Questo contributo fa parte della sezione monografica *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2* – Instant Book, a cura di Gaia Fiorinelli e Matteo Giannelli

---

1. Il Disegno di legge AC 1717 *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici* prevede un ricorso molto significativo allo strumento penalistico, da intendersi, ai fini che qui interessano, come comprensivo di tutte le componenti della complessa filiera che va dalle attività di intelligence *praeter notitiam criminis* all'esecuzione della pena comminata con condanna definitiva. Rinviando ai contributi che precedono per l'esame delle ragioni di fondo e dei contenuti sostanziali di questa scelta di politica criminale nella prospettiva multilivello degli obblighi derivanti, tra gli altri, dal recepimento della c.d. NIS 2 e dalla proposta novella del sistema penale domestico, le riforme riguardanti le più gravi ipotesi di cybercriminalità si pongono in linea di continuità con la tendenza, ormai pluriennale, del legislatore ad estendere l'ambito di applicazione delle disposizioni sostanziali e processuali previste dall'ordinamento per la prevenzione della ed il contrasto alla criminalità organizzata di tipo mafioso ad altre ipotesi di reato parimenti idonee a destare un particolare allarme sociale (si pensi, per limitarsi agli esempi più rilevanti, alla criminalità corruttiva e a quella con finalità di terrorismo). Per meglio comprendere i termini della questione e declinare in maniera conforme al principio generale di tassatività e determinatezza il significato penalistico del predetto riferimento alla *gravità* e all'*idoneità* a destare particolare allarme sociale delle più severe forme di cybercriminalità, giova ricordare come il report *Internet Organised Crime Threat Assessment* (IOCTA) curato dall'*European Cybercrime Centre* (EC3) costituito presso Europol, restituisca, sulla scorta di una complessa elaborazione di informazioni *evidence-based*, la misura e la crescente diffusività di attività criminali che, per complessità, estensione territoriale e potenzialità offensiva nei confronti di vittime individuali, collettive ed istituzionali sono ben lontane dal poter essere commesse da un singolo autore individuale su modello *lonely wolf* essendo, al contrario, riferibili ad una cybercriminalità organizzata sempre più caratterizzata dalla costituzione

e dallo sviluppo di un vero e proprio ecosistema criminale radicato e multiforme. L'ampia casistica esaminata anche grazie all'intensa cooperazione internazionale tra le agenzie di *law enforcement* consente di dar conto della frequente organizzazione di strutture che riflettono il modello della holding operante a livello globale e dedita a varie forme di attività criminali transnazionali grazie ad una struttura ideata, sviluppata e finanziata con un approccio *competence-based* assolutamente inedito ai tradizionali studi ed alle consolidate analisi – anche empiriche - sulla criminalità organizzata di tipo mafioso. L'elevato livello di competenze tecniche richieste per porre in essere le tre principali forme di cybercriminalità organizzata menzionate da Europol, vale a dire i *cyberattacks*, l'*on line fraud* e la *child sexual exploitation*, rende necessario che il *business plan* del gruppo criminale si sviluppi, innanzi tutto, attraverso un vero proprio servizio HR di cui fanno parte i reclutatori di coloro che sviluppano, forniscono e sono in grado di utilizzare tecnologie funzionali alla commissione dei reati. Sono, poi, sviluppate attività, per così dire para-finanziarie che vanno dal *fund raising* all'analisi economica di costi e capacità di produzione di *economic gain* dei reati pianificati. Non mancano, inoltre, competenze più strettamente *legal* volte, anche grazie alla complicità di professionisti in situazioni talvolta limitrofe a quelle del c.d. *grey market* in ragione della possibilità del coinvolgimento di soggetti operanti, anche, in contesti leciti, a fornire ai gruppi criminali consulenze utili ad eludere le indagini delle Autorità competenti e rimodulare con estrema rapidità, ove necessario, i *pattern* di realizzazione dei reati per evitarne l'emersione. Si tratta, come rilevato, di uno schema strutturale in gran parte inedito in quanto caratterizzato, ad un tempo, dalla suddivisione in ruoli tipica dell'associazionismo criminale di tipo mafioso ma anche dalla struttura pulviscolare caratteristica della criminalità organizzata terroristica con una graduazione dell'elemento dell'*intuitus personae*, pure tipico dei gruppi *mafia-type*, a seconda delle esigenze del piano criminale dall'estensione massima che riguarda il consulente che fornisce la tecnologia da utilizzare per la realizzazione dei reati al rilievo minimo dell'hacker che presti in forma anonima i suoi servizi limitando, spesso, il suo coinvolgimento ad un solo segmento dell'*iter criminis*. L'identificazione degli elementi di gravità, per così dire, criminologica di queste forme di cyberorganizzazione illecita si affianca, nel Disegno di legge AC 1717, a presupposti maggiormente riferiti alle vittime come risulta dall'analisi integrata delle disposizioni del disegno e delle leggi complementari variamente richiamate.

2. Traendo le mosse dall'art. 18 del DDL, modificativo dell'art. 13 del d.l. 13 maggio 1991, n. 152 (convertito in legge 12 luglio 1991, n. 203 e recante, per l'appunto, provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa) laddove inserisce il nuovo comma 3-*bis*, emerge la previsione dell'estensione delle disposizioni di cui ai commi 1, 2 e 3 del decreto medesimo relative alla *disciplina delle intercettazioni di conversazioni e comunicazioni* anche quando si procede con riferimento ai delitti, consumati o tentati, previsti dall'art. 371-*bis*, co. 4-*bis* c.p.p. (a sua volta introdotto dall'art. 2-*bis* co. 3, lett. b) del d.l. 10 agosto 2023, n. 105, convertito in l. 9 ottobre 2023, n. 137) per i quali il procuratore nazionale antimafia e antiterrorismo esercita le funzioni di impulso e coordinamento dell'attività nei confronti dei procuratori distrettuali. Si tratta, in particolare, dei procedimenti per i delitti di cui agli artt. 615-*ter*, terzo comma, 635-*ter* e 635-*quinquies* c.p. nonché, «quando i fatti sono commessi in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità», in relazione ai procedimenti per i delitti di cui agli artt. 617-*quater*, 617-*quinquies* e 617-*sexies* c.p. Analoga estensione dello statuto sostanziale e processuale dei delitti in materia di criminalità organizzata si prevede in almeno altri due ambiti paradigmatici della normativa in materia. Il primo è costituito dalla protezione dei collaboratori di giustizia laddove con l'articolo 17 si introducono modifiche al d.l. 15 gennaio 1991, n. 8 prevedendo che le disposizioni aventi ad oggetto il procedimento di assegnazione delle speciali misure di protezione e i benefici penitenziari previsti per i collaboratori ed i testimoni di giustizia di cui al comma 1 (lettere a, b e c) siano estese anche agli autori dei reati informatici modificati o introdotti con il DDL, i quali collaborando con l'autorità giudiziaria si trovino in grave pericolo per le forme di cooperazione attivate o le dichiarazioni rilasciate. A tal ultimo proposito, con l'articolo 20 del Disegno di legge si apportano modifiche alla l.

11 gennaio 2018, n. 6 ed in particolare al comma 2 dell'articolo 11, relativo al procedimento di applicazione delle speciali misure di protezione per i testimoni di giustizia e per gli altri protetti, al fine di prevedere che la Commissione centrale richieda il parere al Procuratore nazionale antimafia e antiterrorismo sulla proposta di ammissione alle speciali misure, non solo per le fattispecie delittuose di cui all'art. 51, commi 3-*bis*, 3-*ter* e 3-*quater* c.p.p., ma anche nel caso di cybercrimes di cui all'art. 371-*bis*, comma 4-*bis* c.p.p. Si prevede, altresì, un allungamento a due anni dei termini di durata massima delle indagini preliminari, oltre che per i delitti di criminalità organizzata, anche per i delitti previsti dagli artt. 615-*ter*, 615-*quater*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 635-*bis*, 635-*ter*, 635-*quater*, 635-*quater*.1 e 635-*quinquies* c.p., «quando il fatto è commesso in danno di sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico». Giova, altresì, menzionare l'estensione ai cybercrimes di cui all'art. 371-*bis*, co. 4-*bis* dei benefici penitenziari di cui all'art. 16-*novies* l. 15 marzo 1991, n. 82 (art. 17, co. 1, lett. c) del DDL). In particolare, si prevede che nei confronti delle persone condannate per uno dei gravi delitti informatici or ora menzionati, analogamente a quanto disposto per i delitti commessi per finalità di terrorismo o di eversione dell'ordinamento costituzionale o per uno dei delitti di cui all'art. 51, co. 3-*bis* c.p.p., possano essere disposte la concessione delle circostanze attenuanti previste dal codice penale o da disposizioni speciali, la liberazione condizionale, la concessione dei permessi premio e l'ammissione alla misura della detenzione domiciliare qualora abbiano prestato, anche dopo la condanna, taluna delle condotte di collaborazione di cui all'art. 47-*ter* del regolamento penitenziario.

3. L'enfasi posta nel Disegno di legge sulla combinazione tra il sensibile innalzamento delle pene edittali e l'estensione dell'applicazione delle disposizioni in materia di indagini preliminari, mezzi di ricerca della prova, processo e misure premiali ai collaboratori di giustizia consente di recuperare, pur se non espressamente emergente dalla formulazione letterale delle disposizioni che lo compongono, il rilievo del carattere "organizzato" degli autori del reato nella selezione, conforme ai principi di tassatività e determinatezza, delle più gravi ipotesi di cybercrimes. Il carattere spiccatamente multiforme e la rapidità ad adattarsi alle necessità poste dall'attuazione del loro piano criminale e delle sempre mutevoli forme di elusione dei controlli operati da parte delle Autorità preposte a livello nazionale e globale rende la segretezza e la complessità dei cybergruppi criminali una sorta di condizione di esistenza e sopravvivenza. Non è infrequente che gruppi criminali diversi collaborino per la realizzazione di alcune attività sfruttando la loro localizzazione geografica e massimizzando la capacità di eludere le investigazioni. Da questo angolo visuale la cybercriminalità organizzata può giovarsi di alcuni *booster* di segretezza che preservano la cifra oscura che affligge questa materia ed ha motivato il rilievo, posto dal DDL, sugli obblighi di segnalazione e denuncia degli attacchi. Si tratta, innanzi tutto, per limitarsi ad uno degli aspetti più significativi, del *dark web* che risulta singolarmente funzionale a supportare l'intero *iter criminis* dalla fase genetica del reclutamento e della ricerca delle tecnologie utili alla commissione dei reati, alla fase in itinere dell'individuazione e del raggiungimento dei target più numerosi di vittime ai, non infrequenti, casi di erogazione di servizi di *continous monitoring* delle attività poste in essere (cross border e non) all'occultamento dei proventi del reato e dei rispettivi responsabili. Emerge, dunque, la necessità di un intervento sinergico e multistakeholder che faccia leva, ad un tempo, sull'emersione degli attacchi, sullo sfruttamento di tutti gli strumenti sostanziali e processuali messi a disposizione dalla legislazione in materia di contrasto alla criminalità organizzata, alla predisposizione di incentivi fino alla concessione di misure di protezione per i casi di dissociazione e alla collaborazione di coloro che, essendo intranei all'organizzazione criminale, possono fornire alle Autorità procedenti informazioni altrimenti difficili da reperire. La predetta scelta di politica criminale si inscrive nel *carrot and stick approach* che, a livello domestico così come europeo ed internazionale, esprime una delle cifre più caratteristiche dell'intervento penale in materia di criminalità organizzata. Non mancano, invero, come anche nella tormentata storia dell'introduzione e delle numerose riforme intervenute nel sistema di contrasto della criminalità organizzata di tipo mafioso, rilievi di ordine generale in merito all'accettabilità, si consenta, etica prim'ancora che giuridica di

un patto volto a favorire la *criminal disclosure* da parte degli autori di gravi reati. Pur non essendo questa la sede per approfondire un tema di tale complessità, l'impianto generale del DDL risulta condivisibile nella ricerca di un sostenibile equilibrio tra la prevenzione delle più gravi forme di cybercriminalità organizzata anche attraverso azioni di capacity building volte ad aumentare la resilienza di tutti i soggetti potenzialmente coinvolti nelle diverse vesti di componenti di agenzie di law enforcement o di potenziali vittime a vari livelli di cybervulnerabilità, l'innalzamento della risposta sanzionatoria sulla scorta della funzione di prevenzione generale negativa della pena e, *last but not least,* l'incentivo a chi sia stato coinvolto nelle più gravi forme di *organized cybercrimes* a dissociarsi e collaborare con l'Autorità procedente. L'approccio multistakeholder risulta, infine, cruciale nel colmare il gap che spesso drammaticamente caratterizza la capacità e la tempestività di *detection* e *reaction* del sistema e l'attitudine dei gruppi criminali a rispondere *real time* agli ostacoli all'attuazione del rispettivo piano criminale. A tale scopo la circolarità del flusso informativo suggerito dall'art. 21 del Disegno di legge appare particolarmente efficace laddove, per un verso, prevede la riforma del comma 4 dell'art. 17 della l. 4 agosto 2021, n. 109 stabilendo che il personale dell'ACN addetto al CSIRT Italia, nello svolgimento delle proprie funzioni, rivesta la qualifica di pubblico ufficiale con la conseguenza che la trasmissione immediata delle notifiche di incidente ricevute all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione costituisce adempimento dell'obbligo di cui all'art. 331 c.p.p. e, per altro verso, che quando acquisisce la notizia dei delitti di cui all'art. 371-*bis*, co. 4-*bis* c.p.p., il pubblico ministero ne dia tempestiva informazione all'Agenzia sempre assicurando il raccordo informativo con l'appena ricordato organo del Ministero dell'interno. L'ambizione risulta, dunque, per quanto specificamente attiene alla prevenzione e al contrasto della cybercriminalità organizzata, quella di un processo di *law enforcement by design* ove, facendo ricorso alle *best practice* del sistema italiano di prevenzione e contrasto della mafia e sfruttando l'innovazione tecnologica sostenuta anche dall'Agenzia per la Cybersicurezza Nazionale, le attività maggiormente a rischio poste in essere dai soggetti potenzialmente più vulnerabili siano *ab origine* svolte, *rectius* disegnate, in modo da essere quanto più resistenti e resilienti ed opporre all'organizzazione criminale un'altrettanta efficace organizzazione della risposta (anche penale) del sistema.

Riferimenti bibliografici

G. Amarelli (2018), *Contiguità mafiosa e controllo penale: dall'euforia giurisprudenziale al ritorno alla legalità*, in G. Acocella (a cura di), "Materiali per una cultura della legalità", Giappichelli, 2018

A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di) (2023), *Cybercrime*, Utet, 2023

A. Di Nicola (2022), *Towards digital organized crime and digital sociology of organized crime*, in "Trends in Organized Crime", May 2022

C. Fijnaut (2008), *Controlling Organized Crime and Terrorism in the European Union*, in M.C. Bassiouni, V. Militello, H. Sarzger (eds.), "European cooperation in penal matters: issues and perspectives", Cedam, 2008

F. Hagan (2006), *"Organized crime" and "organized crime": Indeterminate problems of definition*, in "Trends in Organized Crime", vol. 9, 2006, pp. 127-137

J.B. Jacobs (2020), *The Rise and Fall of Organized Crime in the United States*, in "Crime and Justice", vol. 9, 2020, pp. 17-67

M. Joutsen (2006), *The European Union and Cooperation in Criminal Matters: the Search for Balance*, HEUNI Paper 25, 2006

A. Lavorgna (2020), *Organized crime and cybercrime, in The Palgrave Handbook of International Cybercrime and Cyberdeviance*, Palgrave Macmillan, 2020

S. Lupo (1996), *Mafia*, in "Enciclopedia delle Scienze Sociali", Treccani, 1996

V. Militello, B. Huber (2001), *Towards a European Criminal Law Against Organised Crime. Proposals and Summaries of the Joint European Project to Counter Organised Crime,* Iuscrim, 2001

V. Mitsilegas (2001), *Defining Organised Crime in the EU: the Limits of European Criminal Law in the Area of "Freedom, Security and Justice*, in "European Law Review", vol. 26, 2001

M. Romanelli (2019), *Criminalità organizzata e terrorismo: la circolazione dei modelli criminali e degli strumenti di contrasto*, in "Sistema penale", 20 dicembre 2019

F. Spiezia (2020), *Attacco all'Europa. Un atlante del crimine per comprendere le minacce, le risposte, le prospettive*, Piemme, 2020

E. Viano (a cura di) (2016), *Cybercrime, Organized Crime, and Societal Responses: International Approaches*, Springer, 2016

C. Whelan, D. Bright, J. Martin (2024), *Reconceptualising organised (cyber)crime: The case of ransomware*, in "Journal of Criminology", vol. 57, 2024, n. 1

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0153 • articolo sottoposto a peer review • pubblicato in anteprima il 27 mag. 2024

Stefano Pietropaoli

Un'occasione (forse) mancata. Considerazioni sulla revisione dei reati informatici proposta con il DDL Cybersicurezza

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

Questo contributo fa parte della sezione monografica *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2* – Instant Book, a cura di Gaia Fiorinelli e Matteo Giannelli

Il disegno di legge 1717 propone un'articolata serie di interventi che mirano – anche grazie al rafforzamento delle funzioni dell'Agenzia per la cybersicurezza nazionale (ACN) – a consolidare la sicurezza informatica del Paese.

Mentre le disposizioni di cui al Capo I sono rivolte al conseguimento di una maggiore capacità di protezione e risposta alle emergenze cibernetiche, il Capo II è invece formulato con l'intenzione di garantire una maggiore tutela della persona e del patrimonio di fronte alle ormai diffusissime pratiche criminali svolte sul web (o comunque attraverso strumenti informatici).

Considerato il limitato spazio a disposizione, mi limiterò ad alcune brevi considerazioni generali in riferimento al Capo II, per rilevare poi quelle che mi sembrano le principali criticità del disegno di legge in oggetto.

Prima di tutto, il ddl prevede un generale innalzamento delle comminatorie edittali della quasi totalità dei reati (cosiddetti "necessariamente informatici") introdotti dalla legge 547 del 1993. Si tratta di un inasprimento delle sanzioni, anche molto rilevante, motivato – riprendendo le parole dell'analisi tecnico-normativa che accompagna il ddl – «dall'esigenza di realizzare una più intensa tutela dei beni finali […] fortemente esposti ad allarmanti forme di criminalità informatica».

Questa scelta di fondo appare, in via generale, condivisibile, se si considera il sempre maggiore disvalore delle condotte criminali nello spazio cibernetico. Tuttavia, preme sottolineare che il maggiore problema rappresentato dalle forme di criminalità informatica non consiste tanto nella loro offensività, quanto piuttosto nella effettiva perseguibilità degli illeciti perpetrati. Reati informatici e cybercrimes presentano, come è noto, enormi difficoltà nell'individuazione dei responsabili, che sempre più spesso si avvalgono di raffinate tecniche di offuscamento – VPN, reti Tor, tecnologie di crittografia – capaci di garantire un sostanziale anonimato. Frequentissimi, inoltre, sono gli illeciti commessi a partire da paesi stranieri (con

molti dei quali mancano efficaci accordi di cooperazione giudiziaria).

L'inasprimento delle sanzioni per queste tipologie di illeciti è dunque destinato a rimanere una soluzione insoddisfacente se non accompagnata da misure di diversa natura. Ancor più che nella realtà analogica, nello spazio cibernetico è fondamentale il ruolo della prevenzione. Ma non si ha efficace prevenzione senza conoscenza e consapevolezza. In altre parole, è indispensabile un'attenta opera di pianificazione e promozione di progetti formativi e iniziative di vera e propria "pedagogia digitale" – calibrati sulle diverse fasce di età, istruzione e mansioni – ma rivolti a tutta la popolazione, dalla prima età scolare alla terza età, dall'impiegato al dirigente, dal professionista al pensionato. In particolare, appare urgente prevedere un piano di sviluppo di competenze, strumenti e tecniche che possano rendere più efficace l'azione delle nostre forze dell'ordine, messe in sempre più grave difficoltà da reati davanti ai quali rimangono sostanzialmente impotenti.

Passando a considerazioni di diverso tenore, vorrei esprimere anche qualche perplessità di natura sistematica sull'impianto del ddl 1717.

Il punto più complesso riguarda a mio avviso la proposta di "abrogazione" dell'art. 615-*quinquies* e la sua sostanziale ricollocazione nell'alveo dei delitti di danneggiamento di dati e sistemi informatici ex artt. 635-*bis* e ss.

L'attuale formulazione dell'articolo 615-*quinquies*, effettivamente, ben si può intendere come disposizione normativa che sanziona le condotte dirette a danneggiare o interrompere un sistema informatico o telematico. Pertanto, in questa prospettiva, il suo inserimento quale nuovo art. 635-*quater*.1 è pienamente giustificato (tab. 1).

Testo vigente	Testo ddl 1717
Articolo 615-*quinquies* Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico	Articolo 635-*quater*.1 Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.
«Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329».	«Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici è punito con la reclusione fino a due anni e con la multa fino a euro 10.329».

Tab. 1

La ricollocazione della disposizione vigente ha senz'altro una giustificazione "tematica". Tuttavia, occorre ricordare che la non ottimale collocazione che possiamo riscontrare nel codice vigente è dovuta alle (non felici) riformulazioni – prima con la legge 18 marzo 2008, n. 48 e poi con la legge 23 dicembre 2021, n. 238 – del testo originale.

Occorre infatti ricordare che il legislatore del 1993 aveva effettuato una precisa scelta sistematica: in contiguità con l'articolo 614 (violazione di domicilio), veniva introdotto il reato di "violazione di domicilio informatico" (615-*ter*), accompagnato da altri due illeciti consistenti in condotte prodromiche a tale accesso abusivo: l'art. 615-*quater* e, appunto l'art. 615-*quinquies*.

Credo che sarebbe opportuno sì ricollocare la disciplina dell'attuale art. 615-*quinquies*, ma anche mantenere un reato tematicamente congruente con la scelta del 1993. In altre parole, pur tenendo ferma la ricollocazione del testo del vigente art. 615-*quinquies* come art. 635-*quater*.1, credo sarebbe opportuno modificare (e non abrogare) l'articolo 615-*quinquies* al fine di sanzionare anche le condotte di chi

"si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici", non animato dal dolo specifico di danneggiare illecitamente un sistema informatico o telematico etc., bensì dal dolo specifico di introdursi abusivamente in un sistema informatico o telematico.

Al fine di reintegrare il quadro di tutele originariamente previsto, sarebbe inevitabile il ripristino della disposizione di cui all'art. 615-*quater* alla versione originale.

Cercando di sbrogliare la matassa: ferma restando la ragionevolezza dell'introduzione di un reato (al nuovo art. 635-*quater*.1) che sanzioni, per esempio, l'installazione di programmi allo scopo di danneggiare illecitamente un sistema informatico o telematico, credo che sarebbe altrettanto ragionevole prevedere all'art. 615-*quater* il reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, e al 615-*quinquies* il reato di detenzione, diffusione e installazione di apparecchiature, dispositivi o programmi informatici idonei all'accesso abusivo ad un sistema informatico o telematico.

Senza questo riassestamento complessivo, infatti, rimarrebbe "scoperta" l'ipotesi di chi installi un software malevolo capace di alterare – ma non danneggiare – il funzionamento di un determinato dispositivo con l'unico scopo di consentirne l'accesso abusivo.

Nella tab. 2 riporto, nella colonna di destra, le possibili modifiche agli artt. 615-*quater* e 615-*quinquies*.

Infine, vorrei segnalare l'aspetto che mi sembra più critico nel ddl in esame. Si tratta, in questo caso, della critica non di una nuova previsione, ma dell'assenza di una previsione.

Tra tutti gli illeciti informatici, infatti, quello che rappresenta il maggiore pericolo per la cittadinanza – e che viene commesso con maggiore frequenza – è il fenomeno delle truffe online. Secondo i dati ISTAT, truffa "analogica" e frode informatica ha raggiunto insieme lo straordinario numero di 300.000 denunce inoltrate in un anno all'autorità giudiziaria da parte Arma dei Carabinieri, Polizia di Stato e Guardia di Finanza, a fronte delle 35.000 denunce complessive per gli altri reati informatici.

È tuttavia opportuno sottolineare che il fenomeno comunemente indicato come "truffe online" è estremamente variegato e di non semplice qualificazione sul piano giuridico. Infatti, buona parte delle frodi che avvengono (anche) attraverso l'uso di tecnologie informatiche deve essere inquadrata alla luce della truffa tradizionale di cui all'art. 640 c.p., e non nella diversa fattispecie della frode informatica propriamente detta e prevista dall'art. 640-*ter* c.p.

Soltanto per fare un esempio: chi acquista un bene da un sito internet e si vede recapitato un bene del tutto diverso (e di minor valore) rispetto a quello descritto, subisce una truffa in senso classico. Non rileva, in altre parole, che sia stato tratto in inganno sulla rete. Chi, invece, effettua una operazione bancaria online pensando di operare sul sito del proprio istituto di credito, senza accorgersi di stare operando in realtà su un sito clonato verso il quale è stato indirizzato automaticamente da un *malware* che ha infettato il suo device, subisce il reato di cui all'art. 640-*ter* c.p. nel momento in cui il malfattore riesce a usare quelle credenziali per distrarre una somma di denaro dal suo conto corrente.

Considerata dunque la straordinaria entità del fenomeno, credo che sarebbe opportuno cogliere l'occasione offerta dal presente disegno di legge per ridisegnare l'impianto normativo a presidio dei diritti dei soggetti colpiti da fenomeni fraudolenti.

In particolare, potrebbe essere l'occasione per affrontare un problema rilevante sia sul piano teorico sia sul piano pratico.

Come dimostra in maniera inoppugnabile l'analisi della giurisprudenza in materia, è sempre più complesso – a causa dello sviluppo tecnologico e in particolare dell'impiego degli ultimi esiti dell'intelligenza artificiale – individuare chiari criterî di distinzione tra le fattispecie di cui all'art. 640 c.p. e all'art. 640-*ter*.

Rispetto all'art. 640, il 640-*ter* non richiede l'induzione in errore di un soggetto attraverso artifizi o raggiri. Dottrina e giurisprudenza, dopo una fase che ha fatto emergere orientamenti contrastanti, si sono poi indirizzate in maniera piuttosto decisa verso un'interpretazione che — data l'impossibilità di "trarre in inganno" una macchina che, per quanto "intelligente", non corrisponde ad un essere umano — non considera rilevante ai fini della configurabilità del reato la cooperazione del soggetto tratto in inganno. La frode informatica si caratterizzerebbe dunque rispetto alla truffa in quanto le condotte ad essa riferibili investono non un soggetto passivo, ma un sistema informatico.

Testo vigente	Nuova possibile formulazione
Articolo 615-*quater* Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (L'articolo era originariamente rubricato «Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici». La rubrica è stata modificata dall'art. 19, comma 1, lett. c), l. 23 dicembre 2021, n. 238, che ha introdotto anche alcune modifiche al testo)	Articolo 615-*quater* Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
«Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a due anni e con la multa sino a 5.164 euro».	«Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione fino ad un anno e con la multa fino a euro 5.164».
Articolo 615-*quinquies* Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.	Articolo 615-*quinquies* Detenzione, diffusione e installazione di apparecchiature, dispositivi o programmi informatici idonei all'accesso abusivo ad un sistema informatico o telematico.
«Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329».	«Chiunque, allo scopo di introdursi abusivamente in un sistema informatico o telematico, si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici è punito con la reclusione fino a due anni e con la multa fino a euro 10.329».

Tab. 2

Si tratterebbe pertanto di un reato finalizzato sempre all'ottenimento di un ingiusto profitto con altrui danno, che si concretizza tuttavia specificamente in una condotta illecita intrusiva o alterativa del sistema informatico o telematico (da ultimo si veda Cassazione penale, sez. II, 2 febbraio 2017, n. 9191).

Sta di fatto che la formulazione adottata dal legislatore risulta ambigua sotto diversi profili. La giurisprudenza si è trovata quindi più volte in gravi difficoltà, e un esame anche superficiale delle pronunce sul tema mette in evidenza come casi concreti praticamente identici siano stati a volte inquadrati nell'ambito dell'art. 640 e altre volte in quello dell'art. 640-*ter*. Basti citare la sentenza con cui il Tribunale di Roma (26 febbraio 2016, n. 2787) ha ravvisato la sussistenza del reato di frode informatica nel caso di un soggetto che aveva sottratto le credenziali di una carta di credito al fine di effettuare delle scommesse online, citando a conforto della propria decisione la «pacifica giurisprudenza della Suprema Corte di Cassazione» secondo cui «integra il reato di frode informatica ex art. 640-*ter* del Codice penale, la condotta di introduzione nel

sistema informatico delle Poste italiane mediante l'abusiva utilizzazione dei codici di accesso personale di un correntista e di trasferimento fraudolento, in proprio favore, di somme di denaro, depositate sul conto corrente del predetto». Tuttavia, in casi sostanzialmente identici si è invece sostenuta la sussistenza del reato di truffa, sulla scorta della considerazione che ad essere "raggirato" sembra il titolare della carta di credito più che il sistema informatico.

Ad aumentare ulteriormente la problematicità applicativa della disposizione di cui all'art. 640-*ter* sono i casi che riguardano la clonazione di carte di credito. Intorno a questi esiste un vero e proprio contrasto giurisprudenziale registrato dalla stessa Corte Cassazione (Cassazione penale, sez. II, 14 febbraio 2017, n. 8913), che ha preso atto della difficoltà di qualificare in maniera univoca l'utilizzo indebito di supporti magnetici clonati, potendo essere con validi motivi ricondotto tanto all'indebito utilizzo di carte di pagamento di cui all'art. 493-*ter*, quanto appunto all'art. 640-*ter*.

Pensiamo, infine, al caso emblematico del *phishing*. Questo termine, da un punto di vista giuridico, non è univocamente riferibile all'una o all'altra fattispecie. Mentre, infatti, varianti come lo *smishing* o il *whaling* ricadono nella quasi assoluta totalità dei casi nell'ambito applicativo del tradizionale reato di truffa, il *pharming* o il *tabnabbing* sostanziano condotte invece generalmente riconducibili alla frode informatica.

Allo stato attuale, dunque, la qualificazione giuridica di un atto di *phishing* richiede un esame dettagliato della concreta condotta tenuta dal *phisher*, che di caso in caso può sostanziarsi in forme assai differenti, diversamente sanzionabili, e che a volte rivelano l'impossibilità di una tutela efficace.

Il medesimo problema di inquadramento, infine, è attestato dalle difficoltà nella corretta qualificazione giuridica dei fatti da parte delle forze dell'ordine: numerosissime sono infatti le notizie di reato formulate in maniera non convincente.

In via generale, due sono le strade (e tre le soluzioni) che, mi pare, (potevano e possono) essere intraprese.

La via più semplice: lasciare intatte le formulazioni di cui agli artt. 640 e 640-*ter* del codice penale, inasprendo tuttavia le sanzioni riferibili alla frode informatica. Questa strada – ripeto, la più semplice – non risolverebbe però i problemi

Testo vigente	Testo emendato dalle Commissioni
Art. 640 c.p. Truffa	Art. 640 c.p. Truffa
Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro. La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro: 1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare; 2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità. 2-bis) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5) . Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente.	Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro. La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro: 1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare; 2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità. 2-bis) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5) . 2-*ter*) se il fatto è commesso a distanza attraverso strumenti informatici o telematici idonei a ostacolare la propria o altrui identificazione; Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal secondo comma, a eccezione di quella di cui al numero 2-*ter*.

Tab. 3

di distinzione tra truffa e frode informatica già richiamati.

La versione inizialmente presentata alle Commissioni non prevedeva alcuna modifica delle due disposizioni in questione. Nella versione emendata, invece, viene proposta una modifica del solo art. 640 nel senso riportato in tab. 3.

Temo che, invece di risolvere il problema appena accennato, questa proposta emendata dalle Commissioni possa ulteriormente complicarlo. Questo perché inasprisce la sanzione della truffa 'classica' condotta tramite "strumenti informatici o telematici idonei a ostacolare la propria o altrui identificazione", aggiungendo così un ulteriore fattore di complessità in una materia di per sé già poco chiara. Ferma restando la formulazione dei due articoli – e confermando anche l'incertezza nella distinzione tra truffa e frode informatica – il testo emendato si limita a modificare verso l'alto le comminatorie edittali nel caso in cui il truffatore si serva di strumenti digitali per colpire a distanza. Ma, nella pratica, un caso di *smishing* (che usa come vettore gli sms invece dei messaggi di posta elettronica, sfruttando la minore diffidenza degli utenti nei confronti di una tecnologia avvertita come antiquata e pertanto meno pericolosa) potrebbe rientrare nella previsione di cui al nuovo art. 640 comma 2-*ter*? La risposta, a parere dello scrivente, è tutt'altro che certa. Viceversa: perché una condotta di *pharming* (con cui il truffatore adotta una tecnica di corruzione del Domain Name System, facendo sì che l'indirizzo correttamente digitato dall'utente non venga "risolto" come dovrebbe, ma conduca invece all'apertura di una diversa pagina gestita e controllata dal *phisher*), attuata attraverso "strumenti informatici idonei a ostacolare la propria o altrui identificazione" (come nodi TOR e simili), ricadendo nell'ambito dell'art. 640-*ter*, dovrebbe essere sanzionata in maniera più lieve rispetto al caso di una truffa tradizionale innescata tramite la medesima metodologia? Se l'intento del legislatore è quello di sanzionare in maniera più grave le frodi attuate tramite sistemi capaci di ostacolare l'identificazione del truffatore, pare irragionevole prevedere questo irrigidimento solo per la truffa e non anche per la frode informatica.

Imboccando, invece, la strada della "riforma", si potrebbero sviluppare due soluzioni alternative: una soluzione "di fusione" sarebbe quella di assorbire la frode informatica nella truffa, abrogando l'art. 640-*ter* e adottando una più articolata formulazione del primo comma dell'art. 640 (oltre alla conseguente risistemazione delle attuali aggravanti); in alternativa, si potrebbe adottare la soluzione "del caso aggravato", prevedendo la frode informatica come variante cibernetica del reato di truffa, sulla falsariga della proposta riguardante l'art. 629 (e come già avvenuto per esempio per l'art. 612-*bis*) (tab. 4).

Tutte queste soluzioni presentano vantaggi, svantaggi e conseguenze da ponderare attentamente.

A parere di chi scrive, quella "del caso aggravato" sembrerebbe la più convincente. Da una parte, risolverebbe il problema della distinzione tra truffa e frode informatica, che sarebbero ricondotte ad unità. Dall'altra, rispetto alla soluzione "di fusione", consentirebbe di mantenere una specificità (e una sanzione più grave) nel caso di truffa condotta tramite strumenti informatici (con un aumento di pena pienamente giustificato dalla loro natura subdola).

Nel *cyberspace* siamo tutti più vulnerabili. Per questo motivo, mi sembra una scelta comprensibile quella di aumentare le sanzioni a carico di chi impiega le tecnologie digitali per colpire i punti più deboli della società.

Tuttavia, come già ricordato, questa scelta di politica legislativa non può non essere accompagnata da una più ampia strategia di pedagogia digitale, capace di far penetrare nella cittadinanza l'idea che alcune pratiche di cyber-igiene sono ormai diventate indispensabili per mantenere la salute di quell'organismo complesso, e ancora fragile, che è la società digitale.

Testo vigente	Soluzione "di fusione"	Soluzione del "caso aggravato"
Art. 640 c.p. Truffa	Art. 640 c.p. Truffa	Art. 640 c.p. Truffa
Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro. La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro: 1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare; 2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità. 2-*bis*) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5) . Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente.	Chiunque, con artifizi o raggiri, inducendo taluno in errore, *ovvero alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti*, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro. La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro: 1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare; 2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità. 2-*bis*) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5). Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente.	Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro. La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro: 1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare; 2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità. 2-*bis*) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5) . *2-ter) se il fatto è commesso alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti.* *2-quater) se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema.* *La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.* *Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente.*

Tab. 4

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0144 • articolo sottoposto a peer review • pubblicato in anteprima il 17 mag. 2024

Federico Niccolò Ricotta

Vulnerability disclosure e *penetration testing*: questioni da normare

L'Autore è assegnista di ricerca presso l'IGSG/CNR

Questo contributo fa parte della sezione monografica *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2* – Instant Book, a cura di Gaia Fiorinelli e Matteo Giannelli

1. Nel progressivo impegno legislativo nel campo della sicurezza cibernetica il disegno di legge governativo C 1717 (XIX legislatura) è l'ulteriore tassello utile a blindare lo spazio nazionale e a conformare l'ordinamento interno alle direttive europee.

I profili di intervento sono molti, ma i più convergono sulle modifiche alla legislazione penale in materia di criminalità informatica, responsabilità delle persone giuridiche e competenza della Procura Nazionale Antimafia.

C'è tuttavia un aspetto speculare alle politiche di criminalizzazione ancora non compiutamente trattato ed essenzialmente legato alla dimensione lecita delle attività informatiche offensive realizzate per scopi di sicurezza cibernetica.

Il contesto di riferimento è quello dell'adozione di politiche c.d. di *coordinated vulnerability disclosure* (CVD), espressione con la quale si indica la complessiva regolazione delle pratiche di rilevare, segnalare e gestire le vulnerabilità dei sistemi informatici da parte di sviluppatori, ricercatori e autorità pubbliche.

Tra i vari profili che compongono queste politiche spicca quello della responsabilità di chi controlla la sicurezza dei sistemi: far emergere una vulnerabilità richiede che vengano svolti i c.d. *penetration test*, azioni di sicurezza informatica che possono implicare il ricorso ad attività offensive per saggiare la resistenza di un sistema: per esempio, simulando un attacco come un accesso forzoso ad una rete o un apparato.

Questi stessi test, sebbene siano determinanti nelle prassi di sicurezza, possono essere considerati illeciti ed esporre gli operatori a ripercussioni sul piano penale e civile (per esempio, laddove siano svolti senza il consenso del proprietario del sistema verificato) con potenziali effetti paralizzanti sul piano dello sviluppo e dell'ordinata gestione del fenomeno: da qui, la necessità dell'intervento regolatorio.

2. La fonte del dovere di adottare una politica di CVD è l'art. 12 della direttiva NIS 2.

La direttiva considera le pratiche di *vulnerability disclosure* cruciali per la sicurezza cibernetica e, come tali, da incentivare e regolare (v. i considerando nn. 58 e 60). Sono tracciate allo scopo due

indicazioni alle quali adeguarsi: assicurare ampia e libera partecipazione della comunità di riferimento ma nel contesto di una gestione ordinata della sicurezza cibernetica.

Il richiamo alla partecipazione è piuttosto ricorrente e suggerisce di prediligere politiche nazionali che assicurino il coinvolgimento diffuso e trasparente di tutti i possibili soggetti interessati (sviluppatori, aziende, ricercatori, autorità), soprattutto volgendo un occhio di riguardo alla posizione della comunità tecnico-scientifica che è da porre al riparo dalle conseguenze penali e civili della propria attività. Testimone dell'importanza attribuita alla comunità scientifica e all'indipendenza degli operatori della *cybersecurity* è anche l'invito della medesima NIS 2 (v. considerando 52) a dotarsi di strumenti e applicazioni c.d. *open source*, per dotarsi di processi di sviluppo e verifica più trasparenti e soprattutto "processi di individuazione delle vulnerabilità guidati dalla comunità", quali fattori determinanti per conseguire livelli più elevati di sicurezza.

Sul piano della gestione complessiva del fenomeno, la direttiva imprime comunque una preferenza per un processo accentrato e affidato al coordinamento delle autorità nazionali di settore, affinché le vulnerabilità non siano scoperte e comunicate in modo indiscriminato e potenzialmente dannoso.

Da qui, la prescrizione dell'art. 12 della direttiva di adottare a livello nazionale politiche che consentano alle persone fisiche o giuridiche di rilevare e segnalare in forma anonima le vulnerabilità e adottare le necessarie azioni susseguenti.

Per il vero, lo statuto giuridico di queste politiche è già stato in parte eretto: l'art. 2 del disegno di legge 1717 irrobustisce il dovere di conformarsi alle prescrizioni di sicurezza impartite dall'Agenzia Cyber, che si aggiunge ai doveri di segnalazione di rischi e incidenti già previsti nella normativa primaria.

Restano scoperti, s'anticipava, i profili di responsabilità degli operatori della sicurezza e i relativi meccanismi di tutela.

3. Nella loro dimensione massimalista le politiche di CVD si riassumono nella triade emersione, comunicazione e correzione di una vulnerabilità.

La vulnerabilità è anzitutto un insieme di condizioni che consente la violazione della sicurezza o della riservatezza di un sistema: si sostanzia in una falla nella sicurezza 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, 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 pubblicistico. Questo può accadere, *i.e.*, per quelle dei sistemi che rientrano nel perimetro di sicurezza cibernetica e che, come tali, sono sottoposti alla vigilanza dell'Agenzia per la cybersicurezza nazionale. Questa comunicazione circa l'esistenza della vulnerabilità è l'attività di *disclosure*: in Italia, per esempio, è il CSIRT ad essere destinatario delle informative sui rischi dei sistemi e delle infrastrutture digitali.

4. La *vulnerability disclosure* è così un processo tramite il quale vengono segnalate le vulnerabilità a chi può risolverle, tendenzialmente prima che esse siano rese note al pubblico generale. Questo processo, quindi, consente a venditori, sviluppatori, gestori e ricercatori IT di cooperare per trovare soluzioni che riducano il rischio associato alle vulnerabilità: un ricercatore, colui che trova che scopre un difetto in un sistema, informa lo sviluppatore (venditori, fornitori) del sistema riguardo al difetto e alle possibili correzioni, affinché quest'ultimo possa assumere misure di mitigazione (patch, monitoraggio del traffico, blocco) per eliminare o ridurre il rischio associato alla vulnerabilità.

5. Le falle nella sicurezza informatica emergono perché vengono condotti i c.d. *penetration test*, pratiche che simulano un attacco ad un sistema per identificarne le debolezze. I test possono essere svolti da soggetti interni alla società che sviluppa il sistema, oppure da esterni, soggetti pubblici o privati (come enti di ricerca o organizzazioni no profit), che operano con o senza la consapevolezza ed il consenso delle entità proprietarie dei sistemi.

Per questo tali attività, così come gli strumenti utilizzati per i test, possono costituire una condotta illecita penalmente o civilmente rilevante. 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 (o le amministrazioni) a non far emergere pubblicamente i difetti dei propri

prodotti e, quindi, a non consentire che siano i terzi a condurre i *penetration test*.

6. I profili di rilevanza penale, comuni alla persona fisica e a quella giuridica (quest'ultima ne risponde nei limiti della responsabilità *ex* d.lgs. n. 231/2001), riguardano l'attività di emersione e, in misura minore, quella successiva della comunicazione.

Quanto all'emersione, tanto la materiale esecuzione del test quanto talune delle attività preparatorie possono avere conseguenze penali: il test può integrare una delle condotte che puniscono l'accesso, lo svolgimento di operazioni abusive ai sistemi informatici o la manipolazione dei dati senza autorizzazione (così agli artt. 615-*ter* c.p., 617-*bis* c.p., 635-*bis* – art. 635-*quinquies* c.p.); del pari, anche l'approvvigionamento delle apparecchiature necessarie a condurre il test può integrare uno dei reati che puniscono procacciamento, detenzione e uso di certi *software* che la legge ritiene pericolosi (come i programmi c.d. *dual use*, così all'art. 461 c.p., artt. 625-*quater* e *quinquies* c.p, art. 617-*quinquies* c.p., ma anche artt. 171-*bis* e *ter* della l. 22 aprile 1941, n. 633, c.d. Legge sulla protezione del diritto di autore).

In tutte queste fattispecie assume rilevanza la violazione della volontà del titolare del sistema informatico che, in forza del proprio *ius excludendi alios*, potrebbe non autorizzare l'accesso ai propri sistemi o risorse da parte di soggetti diversi dai propri. Da qui, il fondamento di una responsabilità che prescinde dai motivi del soggetto agente e/o dalla natura dei programmi, dei dati o delle informazioni archiviate o trattate nel sistema informatico, ovvero dai "risultati" o dalle "conseguenze" del fatto.

Ulteriormente, sul piano della comunicazione, una *disclosure* della vulnerabilità potrebbe integrare il reato di diffamazione se le informazioni sulle possibili criticità del sistema giungono incontrollate al pubblico.

Va da sé che, per entrambi i profili, la responsabilità penale è accompagnata dalle possibili pretese di natura risarcitoria nutrite dai titolari dei sistemi violati.

7. Dati i termini della problematica, può essere utile guardare alle soluzioni già sperimentate altrove. Ad oggi sono quattro gli Stati membri dell'Unione europea, Francia, Olanda, Lituania e Belgio, che hanno proceduto a introdurre policy di CVD e a regolamentare la responsabilità penale, prevedendo forme di *safe harbour* per i tester.

Tra questi, è interessante dare atto dell'equilibrio raggiunto dalla Repubblica Francese, dove una modifica introdotta all'art. 40 del codice di procedura penale consente al pubblico ministero di non esercitare l'azione penale nei confronti del *penetration tester*.

Le condizioni dell'inazione sono poste dagli art. 47 della Legge per una Repubblica Digitale (LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique) e dall'art. L 2321-4 *Code de la defense*: i ricercatori che segnalano una vulnerabilità devono agire in buona fede, nella consapevolezza di star procedendo legalmente e secondo i regolamenti di settore; la vulnerabilità deve essere segnalata tempestivamente ed esclusivamente all'ANSSI (*Agence nationale de la sécurité des systèmes d'information*) l'autorità nazionale francese per la cybersicurezza, che a sua volta garantisce l'anonimato del segnalante e la riservatezza delle condizioni di scoperta del vulnerabilità (così da tutelare le aspettative di tutti i soggetti coinvolti).

Così, soddisfatto l'onere di comunicazione all'autorità di settore, il pubblico ministero può valutare autonomamente la meritevolezza dell'attività del *pen tester* e, se del caso, non promuovere l'azione penale nei suoi confronti.

8. In sé per sé considerata, la soluzione francese è una scelta incentivante perché l'esenzione da responsabilità è essenzialmente processuale, e dipende dalla scelta discrezionale del PM di non procedere se ritiene l'attività del tester conforme a buona fede. A sua volta, in questo giudizio che la Procura conduce sulla meritevolezza dell'azione del tester confluisce anche quello sulla diligenza nell'attenersi alle indicazioni dell'autorità governativa di settore: tanto in termini di aderenza ai regolamenti adottati, tanto nell'esauriente trasmissione dei dati relativi alla propria attività di test. Così, l'esenzione di responsabilità opera in sinergia tra il piano penale e quello regolatorio.

Va da sé che in Francia l'azione penale è discrezionale: è per questo che la loro soluzione può contemplare una valutazione dell'agito del tester condotta secondo criteri così elastici.

9. *De iure condendo*, raggiungere un equilibrio analogo in Italia è un'operazione decisamente più difficoltosa. Una politica normativa CVD che contempli l'area del penalmente rilevante deve infatti

conformarsi ai principi di stretta legalità e dell'obbligatorietà dell'esercizio dell'azione penale (che ne è conseguenza).

Ipotizzando quindi un'area di esenzione da responsabilità satisfattiva delle aspettative della NIS 2 ma coerente con il sistema italiano, una soluzione papabile potrebbe essere quella di coniare una scriminante o una condizione di non punibilità per determinante attività del *penetrator tester*. Così procedendo, la conseguenza sul piano processuale sarebbe quella di promuovere l'archiviazione del procedimento penale o il proscioglimento dell'imputato con riflessi, laddove si operasse sull'antigiuridicità, anche sull'eventuale responsabilità civile.

Ai fini di una qualsiasi esimente, discernere le attività illecite da quelle lecite, e di conseguenza valutare la meritevolezza dell'attività del tester per esentarlo da responsabilità, richiede parametri oggettivi e condizioni poste dalla legge: *i.e.* individuando le condotte rilevanti e in quale proporzione l'offesa arrecata dal test può dirsi giustificata per perseguire obiettivi di sicurezza cibernetica, conferendo eventualmente rilevanza al grado di conformità della condotta dell'agente alle linee guida di settore e, più in generale, ai doveri nei confronti dell'Agenzia nazionale di settore.

Dal punto di vista soggettivo, andrebbe inoltre considerata la diversa situazione di chi svolge attività istituzionali di sicurezza da quella dei privati.

Per il personale in ruolo all'ACN o delle forze di polizia risulta decisamente più semplice disegnare una scriminante speciale in ragione della rilevanza delle proprie funzioni di sicurezza che, sebbene in situazioni diverse, sono già assistite da esimenti penali (si pensi, *i.e.*, alla disciplina dell'agente sotto copertura ex art. 9 legge 16 marzo 2006, n. 146 o quella delle c.d. garanzie funzionali).

Diversamente, per i privati, siano essi persone fisiche o giuridiche, si deve soddisfare l'esigenza di promuovere l'indipendenza della ricerca e l'anonimato della segnalazione (art. 12 NIS 2) senza tuttavia giungere ad una liberalizzazione incontrollata di condotte pur sempre potenzialmente decettive, che potrebbero ben prestarsi ad usi strumentali o obliqui (incentivati da uno scudo penale troppo ampio).

Da qui, la necessità di considerare, anche ai fini dell'esenzione da responsabilità, il rispetto di obblighi regolamentari e amministrativi che consentono un'ordinata e consapevole gestione della sicurezza cibernetica da parte dell'Agenzia, l'organo così deputato a fornire le indicazioni guida e a verificare le circostanze delle attività di sicurezza potenzialmente offensive.

10. Come si è visto, nel disegno di legge governativo C 1717 la questione della *vulnerability disclosure* non è stata ancora compiutamente regolata.

Tuttavia, l'assenza di normazione degli ulteriori profili, soprattutto quelli che insistono sulla responsabilità penale, non deve sorprendere: le politiche di CVD sono una problematica piuttosto complessa da risolvere, in parte per questo dualismo tra la dimensione lecita e illecita ma soprattutto per le numerose implicazioni che esso comporta sul piano dei diritti privati e su quello della sicurezza pubblica.

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0137 • articolo non sottoposto a peer review • pubblicato in anteprima il 4 apr. 2024

Antonio Iannuzzi

Considerazioni sul disegno di legge «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717)

Audizione informale innanzi alle Commissioni riunite I (Affari costituzionali) e II (Giustizia) della Camera dei Deputati

Si pubblica il testo dell'audizione orale svolta il giorno 28 marzo 2024 presso la Camera dei Deputati, Commissioni permanenti riunite I (Affari costituzionali) e II (Giustizia), sul disegno di legge in materia di «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717). Sono qui avanzate considerazioni sull'impianto generale della proposta e su alcune disposizioni del disegno di legge.

Cybersicurezza – Resilienza – Direttiva NIS 2 – Pubblica amministrazione – Reati informatici
Agenzia per la Cybersicurezza Nazionale (ACN)

Notes on the bill on "Provisions on strengthening national cybersecurity and cybercrimes" (AC 1717)

Oral hearing at the Chamber of Deputies, Joint Standing Committees I (Constitutional Affairs) and II (Justice)

The text of the oral hearing held on March 28, 2024 at the Chamber of Deputies, Joint Standing Committees I (Constitutional Affairs) and II (Justice), on the bill on "Provisions on strengthening national cybersecurity and cybercrimes" (AC 1717) is published. The text suggests some considerations about the general outline of the proposal and some provisions of the bill are advanced here.

Cybersecurity – Resilience – NIS 2 – Public Administration – Cybercrimes
Italian Agency for National Cybersecurity

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

Questo contributo fa parte della sezione monografica *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2* – Instant Book, a cura di Gaia Fiorinelli e Matteo Giannelli

Onorevole Presidente, onorevoli Deputati,

1. Il disegno di legge «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (A.C. 1717) è stato presentato come una risposta sostanziale all'aumento delle minacce derivanti da attacchi cibernetici e, dal Presidente del Consiglio dei ministri, come una risposta politica al grave c.d. "caso dossieraggi", emerso a seguito del fatto che la Procura di Roma ha accertato che un ufficiale della Guardia di finanza, distaccato presso la Direzione nazionale antimafia, era responsabile di numerosissime interrogazioni al Sistema dell'Agenzia delle entrate riguardanti diversi politici italiani.

2. La prima parte del provvedimento è sostanzialmente un'anticipazione della normativa di recepimento della Direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (NIS 2) all'interno dell'ordinamento italiano, con l'obiettivo di «sviluppare capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici». Alcune previsioni sono significative e senza dubbio da apprezzare positivamente: le nuove norme, infatti, vanno ad individuare un "superperimetro" che comprende al suo interno sia i soggetti destinatari delle misure previste dalla Direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (NIS 1), sia i soggetti inclusi nel Perimetro di Sicurezza Nazionale Cibernetica, sia altre entità che vengono esplicitamente elencate e che non appartengono a queste categorie. Proprio questo elemento ulteriore è molto interessante perché affronta alcune linee di presidio attualmente scoperte (anche se in prospettiva coperte dalla Direttiva NIS 2): i comuni sopra i 100.000 abitanti, e, comunque, i comuni capoluoghi di regione, e le rispettive *in-house* e poi le società di trasporto pubblico locale con analogo bacino.

2.1. Con riguardo all'obbligo per i Comuni con popolazione superiore ai 100.000 abitanti e, comunque, dei comuni capoluoghi di regione, soggetti all'obbligo di segnalare e notificare gli incidenti indicati nella tassonomia di cui all'art. 1, co. 3-*bis*, del d.l. 21 settembre 2019, n. 105, aventi impatto su reti, sistemi informativi e servizi informatici di rispettiva pertinenza, sono da segnalare due ordini di questioni.

La prima cosa da osservare è, secondo i dati statistici disponibili, che i Comuni oltre i 100.000 abitanti sono oltre 40; ad essi andranno ad aggiungersi i capoluoghi di regione con popolazione inferiore. Sulla reale capacità dei Comuni di far fronte, con rapidità ed efficienza, a quest'obbligo si possono nutrire dei dubbi, alla luce peraltro della presumibile carenza in organico di figure con simile professionalità. Il depauperamento della dotazione organica dei Comuni e delle Città metropolitane che si è determinato negli ultimi anni si rende ancora più evidente per i profili ad alta specializzazione tecnica. In conseguenza di queste criticità, si potrebbero incentivare sia una gestione associata, nella forma di convenzioni, sia la possibilità di gestione come "unione di comuni", nel caso di Comuni limitrofi, stante il fatto che la disciplina legislativa in tema di unione di comuni, l'art. 32 del TUEL a livello statale e le leggi regionali, non dettano limiti specifici relativamente agli ambiti di intervento. Si potrebbe, anche, pensare di valorizzare l'assistenza fornita dall'ANCI.

Consentitemi, però, di rilevare criticamente che il ddl prevede la clausola dell'invarianza finanziaria che mal si concilia con le enormi esigenze di formazione sia di nuove professionalità esterne all'amministrazione sia di personale amministrativo già nei ruoli che potrebbe essere riqualificato all'uopo. La mancanza di formazione sulla sicurezza cibernetica, che è parte di un deficit di conoscenze digitali dei cittadini italiani, deve essere assunta come un'emergenza democratica ed una questione costituzionalmente rilevante. Il *Digital*

Economy e Society Index (DESI) 2022 – indice che misura lo sviluppo dell'economia e della società digitale stilato annualmente dalla Commissione europea – colloca l'Italia nell'indecorosa posizione del 25° posto fra i 27 paesi aderenti all'Ue alla voce capitale umano, con un disarmante tasso di analfabetismo digitale pari a più della metà della popolazione, in quanto solo il 46% degli italiani risulta in possesso di competenze digitali di base. Oggi il PNRR sta investendo nell'acquisizione di competenze digitali, ma occorre preoccuparsi di assicurare una formazione continua dopo la fine del PNRR, non solo garantendo investimenti finanziari, ma anche reimmaginando i soggetti che saranno deputati ad erogare tali saperi, tenendo in considerazione che la formazione professionale è da lungo tempo un elemento di criticità in Italia.

Sotto questo profilo è da apprezzare l'iniziativa dell'Agenzia per la cybersicurezza nazionale (ACN) che con l'Avviso n. 8/2024 ha avviato una procedura per la selezione di proposte di interventi di potenziamento della resilienza cyber dei grandi Comuni, dei Comuni capoluogo di Regione, delle Città Metropolitane, delle Agenzie regionali sanitarie e delle Aziende ed enti di supporto al Servizio Sanitario Nazionale, delle Autorità di sistema portuale, delle Autorità del Bacino del Distretto idrografico e delle Agenzie regionali per la protezione dell'ambiente. Si tratta, comunque, di risorse stanziate «a valere sul PNRR», per cui resta la mancanza di previsione di risorse ordinarie per la formazione del personale e per favorire il percorso di accompagnamento delle amministrazioni all'adeguamento agli obblighi previsti.

La seconda cosa da osservare riguarda la circostanza che i Comuni indicati all'art. 1 dovranno anche individuare, ai sensi dell'art. 6, comma 2, «il referente per la cybersicurezza», selezionandolo «in ragione delle qualità professionali possedute». In merito occorre segnalare che la previsione normativa, così come genericamente formulata, non consente di individuare con sicurezza i requisiti professionali di cui dovrà essere in possesso detto referente (attestazioni, certificazioni, pregressa esperienza, che tipo di formazione accademica?) Se si pensa di individuare una figura equivalente al *Chief Information Security Officer* (CISO) previsto dalla NIS 2 per le aziende, allora occorre far mente che il CISO deve possedere una competenza solida e consolidata nel campo delle tecnologie informatiche e dei concetti basilari della sicurezza informatica. Di solito, il CISO ha una formazione accademica in informatica, ingegneria informatica o un settore affine. Deve aver accumulato esperienza pratica nella supervisione della sicurezza informatica ed aver acquisito una conoscenza approfondita delle normative e degli standard di sicurezza, quali principalmente la certificazione ISO 27001. Non è neppure chiaro, stante la laconicità della norma, se l'amministrazione dovrà istituire una struttura interna, con il coordinamento del referente per la cybersicurezza. Questi dubbi probabilmente consigliano l'inserimento di una previsione che demanda ad un successivo decreto la chiarificazione di questi aspetti, che appaiono di primaria importanza se si pensa alle funzioni attribuite al referente ed alle sanzioni in cui possono incorrere i Comuni. Occorre tenere in considerazione che di una chiarificazione relativa alle qualità professionale del referente beneficerebbero tutte le amministrazioni individuate all'art. 1 del ddl in discussione, che sono soggette al medesimo obbligo.

Ancora, sarebbe opportuno valutare se dal punto di vista funzionale tale referente possa essere inquadrato come dirigente, sia in ragione dei maggiori poteri di intervento, sia per attivare la connessa responsabilità dirigenziale in caso di inadempienza.

2.2. In riferimento all'inclusione delle società *in house* appare necessario chiarire il tema delle *in house*, anche in prospettiva NIS 2. La mera partecipazione azionaria, infatti, non è un criterio efficace per l'inserimento nel perimetro di sicurezza nazionale, che invece è più influenzato dal settore di attività e dall'oggetto del servizio più che dalla forma giuridica che connota il rapporto tra comune e soggetto imprenditoriale (*in house*). In particolare, si dovrebbe far riferimento a tutti i servizi esternalizzati, a prescindere se essi siano esternalizzati nella formula dell'*in house providing* o meno. Peraltro, la dicitura «in house» rischia di essere equivoca e di non richiamare in maniera definita una precisa ed unica fattispecie. Meglio sarebbe riferirsi alle società affidatarie o concessionarie di servizi essenziali, escludendo invece società *in house* che potrebbero essere affidatarie di servizi non particolarmente critici o comunque non inclusi nella direttiva NIS 2.

3. Relativamente ai poteri dell'Agenzia per la cybersicurezza nazionale ed ai successivi obblighi per i

soggetti di cui all'art. 1, comma 1 il ddl prevede, in particolare all'art. 2, che i soggetti destinatari degli obblighi «in caso di segnalazioni puntuali dell'Agenzia per la cybersicurezza nazionale circa specifiche vulnerabilità cui essi risultino *potenzialmente* [corsivo mio, n.d.a.] esposti, provvedono, senza ritardo e comunque non oltre quindici giorni dalla comunicazione, all'adozione degli interventi risolutivi indicati dalla stessa Agenzia».

Il secondo comma aggiunge che «La mancata o ritardata adozione degli interventi risolutivi di cui al comma 1 comporta l'applicazione delle sanzioni di cui all'articolo 1, comma 5, salvo il caso in cui motivate esigenze di natura tecnico-organizzativa, tempestivamente comunicate all'Agenzia per la cybersicurezza nazionale, ne impediscano l'adozione o ne comportino il differimento oltre il termine indicato al comma 1».

Tale formulazione normativa merita di essere chiarita.

In primo luogo, potrà essere valutata l'opportunità di espungere il riferimento alla potenziale esposizione («potenzialmente esposti») giacché la sottoposizione a sanzione sembra presupporre l'accertamento di una condizione certa di esposizione al pericolo.

In secondo luogo, non appaiono sufficientemente determinate le «motivate esigenze di natura tecnico-organizzativa», che se «tempestivamente comunicate all'Agenzia per la cybersicurezza nazionale», possono comportare il differimento del termine o finanche la mancata adozione delle misure risolutive indicate dall'ACN. Il rischio è che una formulazione così generica possa essere troppo facilmente addotta finendo per stemperare, fino a vanificare, l'imposizione dell'obbligo. È vero che l'ACN potrà sindacare le motivazioni, ma la formula non contiene alcuna specificazione riguardo alle esigenze di natura organizzativa che giustificano il tardivo o mancato intervento, tuttavia essa appare foriera di contenzioso. Avverso la sanzione, infatti, entro 30 giorni dalla sua notificazione l'interessato può presentare opposizione all'ordinanza ingiunzione (che, di regola, non sospende il pagamento), inoltrando ricorso all'autorità giudiziaria competente (artt. 22, 22-*bis*, l. 24 novembre 1981, n. 689).

4. Sia consentito, a questo punto, un breve inciso sull'impianto generale del disegno di legge, che è scritto con un metodo tutto incentrato sull'individuazione di obblighi a cui corrispondono sanzioni, ora più severe. Questa impostazione a mio avviso non favorisce l'acquisizione di una cultura della cybersicurezza che presuppone la maturazione della consapevolezza che il rafforzamento della sicurezza cibernetica è un vantaggio per il Paese e che è interesse comune adoperarsi per la sicurezza delle reti. È importante notare che diverse disposizioni incluse in questo ddl, ma lo stesso vale per molte disposizioni presenti anche nella Direttiva NIS 2 che si andrà presto a recepire, riflettono le pratiche di sicurezza informatica che la maggior parte delle organizzazioni pubbliche o private dovrebbe implementare per proteggere sia i dati dei cittadini sia, per le aziende, il proprio business. Di conseguenza, le amministrazioni, in questa fase, dovrebbero progressivamente mirare a elevare i requisiti minimi in materia di sicurezza informatica, dedicando risorse finanziarie e competenze necessarie a tale scopo. La capacità di riconoscere rapidamente la natura di un attacco e di adottare misure efficaci per mitigare il rischio diventa un aspetto cruciale per garantire l'efficacia dei sistemi di sicurezza informatica e la preparazione dei dipendenti, i quali dovrebbero essere costantemente formati per sviluppare e migliorare le loro pratiche di sicurezza informatica nel tempo. Pertanto, in un mercato con limitate risorse professionali come quello della sicurezza informatica, diventa sempre più decisivo orientare le strategie e gli investimenti verso la formazione di personale qualificato e sempre aggiornato.

5. La seconda parte del ddl è relativa all'incremento delle pene per i *cyber crime* oltre a creare nuove fattispecie di reato. Tra queste particolarmente rilevante è il tema di cui all'art. 1, lettera *p*), che introduce l'art. 635-*quater*.1 del Codice penale, per la disciplina del reato di «Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico».

L'articolo rischia di determinare, nella formulazione attuale, alcuni problemi interpretativi.

Mi soffermo sulla questione principale: è necessario che venga meglio chiarito e specificato il concetto "danneggiare illecitamente", che indurrebbe a pensare che esista – e che quindi sia legittima – l'ipotesi di "danneggiare lecitamente".

In molti casi l'attività di cybersecurity potrebbe portare a svolgere talune delle attività di sopra richiamate, ma non a scopo malevolo, bensì a

scopo difensivo. Tuttavia, se questo era l'intento del proponente, la formulazione non è certamente delle più chiare ed immediate, soprattutto se pensiamo al fatto che, nell'ordinamento italiano, non è prevista la legittima difesa cibernetica.

Proprio questo può essere il punto di svolta del provvedimento: il riconoscimento del legittimo ricorso all'uso del mezzo informatico per difendersi da una azione violenta che metta a rischio la sicurezza del singolo o di altri ovvero i beni ovvero il domicilio, sebbene digitale. L'esempio concreto è quello di un *Red Team* (difesa attiva) che agisca per far cessare un attacco informatico, che potrebbe incorrere nel reato – non essendo disposta la fattispecie del "danneggiamento lecito" – per danneggiamento illecito delle capacità dell'*hacker*. Ancora, il servizio di *Cyber Threat Intelligence* che recupera nel dark web informazioni che consentono di sventare un attacco informatico potrebbe incorrere nella fattispecie dell'"abusivamente si procura", anch'essa prevista dal ddl, non essendo definito quando sia invece consentito il "procurarsi" dati, informazioni ecc. E così di seguito.

L'assetto normativo nuovo, soprattutto, potrebbe mettere a rischio la professione e l'attività di *penetration testing*. Quella cioè in cui un soggetto viene ingaggiato per testare, attraverso un attacco concordato, le difese di un sistema informatico. Anche in quel caso vi sono condotte "offensive" non supportate però da un intento doloso. Certamente non si vuole vietarle, ma il rischio è quello di determinare un'inversione dell'onere della prova in relazione allo "scopo" per il quale si detiene una determinata capacità o si effettua una determinata azione.

Mi chiedo se in tal modo il legislatore intenda estendere la portata dell'art. 52 del Codice penale in tema di legittima difesa. A mio avviso, nel solco della giurisprudenza costituzionale più recente, è possibile ampliare interpretativamente la tutela costituzionale e legislativa del domicilio, di modo che domicilio analogico e digitale possano essere tutelati allo stesso modo dalla legge, così come avviene per la nozione di corrispondenza. La sentenza n. 170/2023 della Corte costituzionale ha esteso, infatti, la nozione di "corrispondenza", nel caso di specie proprio per l'estensione delle prerogative dei parlamentari *ex* art. 68, co. 3, Cost., alle «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». Insomma, muta lo spazio di applicazione, non il diritto in oggetto.

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0136 • articolo non sottoposto a peer review • pubblicato in anteprima il 4 apr. 2024

Erik Longo

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

Il testo sviluppa l'audizione orale svolta il giorno 28 marzo 2024 presso la Camera dei Deputati, Commissioni permanenti riunite I e II, sul il disegno di legge in materia di «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717). Sono svolte una serie di considerazioni sulla portata e delle disposizioni del disegno di legge e su alcuni aspetti che potrebbero richiedere un'attività emendativa durante le fasi di approvazione parlamentare.

Cibersicurezza – Resilienza – Direttiva NIS 2 – Pubblica amministrazione – Reati informatici – CSIRT

Oral hearing on the bill on "Provisions on strengthening national cybersecurity and cybercrimes" (AC 1717)

Chamber of Deputies, Joint Permanent Committees I and II - Rome, 28 March 2024

The paper develops the oral hearing held on 28 March 2024 at the Chamber of Deputies, Joint Permanent Committees I and II, on the bill on "Provisions on strengthening national cybersecurity and cybercrimes" (AC 1717). A number of considerations are made on the scope and provisions of the bill and on some aspects that may require amendments during the parliamentary approval stages.

Cybersecurity – Resilience – NIS 2 Directive – Public Administration – Cybercrimes – CSIRT

L'Autore è professore associato di Diritto costituzionale presso l'Università di Firenze

Questo contributo fa parte della sezione monografica *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2* – Instant Book, a cura di Gaia Fiorinelli e Matteo Giannelli

Sommario: 1. Introduzione. – 2. Introdurre la cultura della cybersicurezza. – 3. Considerazioni generali. – 4. Commenti puntuali.

1. Introduzione

Ringrazio i Presidenti e gli onorevoli membri delle Commissioni I e II per il gentile invito a prendere parte a questo ciclo di audizioni sul disegno di legge in materia di «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717). Le mie osservazioni provengono dalla lettura del testo del disegno di legge e dal Dossier che è stato preparato dai servizi studi congiunti di Camera e Senato. Ho avuto modo di leggere alcune delle memorie depositate e ascoltare le ricche audizioni svolte fino ad ora.

Il primo dato che vorrei sottolineare, e che rappresenta un punto di partenza necessario per ragionare sul disegno di legge odierno, è che ci troviamo in un momento del tutto particolare della storia, nel quale affrontare nuove norme sulla cybersicurezza rappresenta una decisione politica che attiene alla sostanza della sovranità dello Stato italiano, tanto nella sua dimensione interna quanto nella sua dimensione esterna[1].

La cybersicurezza oggi interessa tutti e non solo gli esperti. Non si tratta più solo di una questione legata all'intelligence o alla messa in sicurezza di alcuni dispositivi che possono essere infettati da "malattie" informatiche. La vita digitale ci espone in ogni momento a nuove minacce dovute tanto a errori quanto a comportamenti intenzionalmente malevoli[2].

L'esigenza di protezione dal rischio di un attacco informatico e dai danni che ne possono derivare, riassunta nel termine "cyber-resilienza", sta spingendo molti paesi del mondo a concepire in maniera diversa la sicurezza stessa, e quindi le dinamiche di potere che a essa si riferiscono.

L'ultimo rapporto del Clusit[3] riporta che dal 2018 abbiamo assistito a un aumento del 61,5% a livello mondiale e del 300% nel nostro Paese di attacchi arrivati a buon fine. Gli attacchi ransomware sono cresciuti del 41% nel 2022. Anche gli attacchi via e-mail, compreso il phishing, sono aumentati del 48% nel 2022. Gli attacchi hanno iniziato a concentrarsi anche sull'interruzione delle catene di approvvigionamento, già perturbate a seguito della pandemia e ancor più dopo l'inizio della guerra in Ucraina.

Il costo di questi incidenti sta salendo alle stelle. Uno studio del *Joint Research Center* dell'Ue[4] ha stimato che il costo globale della criminalità informatica ha raggiunto una cifra che supera i 5 trilioni di euro, rispetto ai 2,7 trilioni di euro del 2015. La stima per il 2025 è di 10,5 trilioni di dollari. Il costo medio globale di una violazione dei dati nel 2022 è stato stimato in 4,35 milioni di dollari. L'agenzia europea ENISA evidenzia che aziende e istituzioni europee spendono il 41% in meno per la sicurezza informatica rispetto agli Stati Uniti.

2. Introdurre la cultura della cybersicurezza

In tale ottica diviene essenziale non solo garantire servizi ed evitare danni ma anche diffondere il più possibile la cultura della cybersicurezza, come indicato dalla stessa Strategia nazionale

1. Serini 2023.
2. Brighi 2017.
3. Clusit 2024.
4. Gianmarco-Josefa-Stephane et al. 2020.

2022-2026[5]. È quanto mai opportuno promuovere una profonda consapevolezza in tale materia, sottolineando l'importanza cruciale che le minacce digitali assumono nella salvaguardia degli interessi strategici della nazione e nell'incolumità del tessuto produttivo, con un focus particolare sulle vulnerabilità che interessano le amministrazioni, da un lato, e le piccole e medie imprese, dall'altro.

Al fine di elevare il livello di sicurezza informatica e di assicurare una resilienza ottimale di fronte alle minacce cibernetiche, si rende necessario accompagnare norme che impongono obblighi alla predisposizione di strumenti che consentono agli enti e alle imprese di mappare le proprie vulnerabilità e di conoscere da dove possono venire le minacce, con l'obiettivo di fornire una guida concreta per la prevenzione, il rilevamento precoce, la risposta efficace e la ripresa rapida in caso di attacchi informatici. La realizzazione di un simile paradigma di sicurezza richiede un impegno congiunto e coordinato tra gli attori pubblici e privati, un continuo aggiornamento tecnologico e formativo, nonché una costante vigilanza e adattamento alle evoluzioni del panorama delle minacce cibernetiche.

Questo disegno di legge meritoriamente cerca di rafforzare tanto la risposta penale alle minacce alla sicurezza informatica quanto la resilienza della pubblica amministrazione, anticipando e in un certo qual modo mettendo un "punto fermo" nazionale prima della attuazione della Direttiva 2022/2555 c.d. NIS 2. Come si legge nell'art. 6 della Direttiva, le nuove norme si applicano solo agli enti della pubblica amministrazione a livello centrale. Sono poi gli Stati membri a decidere se estenderle agli enti anche a livello regionale e locale. I problemi di coordinamento delle norme odierne con l'attuazione della NIS mi paiono il problema più rilevante di questo disegno di legge; un problema di fondo che può minare l'efficacia e il risultato sperato dal legislatore. A questo fine, il testo che segue proverà a fornire un quadro composto di tre considerazioni generali e poi tre commenti puntuali.

3. Considerazioni generali

La *prima* osservazione generale attiene alle norme repressive dei fenomeni criminosi. Sono state già svolte molte considerazioni sul punto. Mi limito solo a sottolineare, come è stato già fatto da altri, che la deterrenza sanzionatoria non sempre colpisce nel segno[6]. Semmai essa indica la riconosciuta insidiosità di tali reati e la correlata aggressione a beni giuridici di preminente interesse nella scala costituzionale dei valori. Eviterei di limitarsi ad aumentare le pene senza farne un'occasione per intervenire sui potenziali punti deboli della disciplina, evidenziati da molto tempo da parte della dottrina (anche ultimamente con riguardo al recepimento della Direttiva 2013/40/UE).

Aggiungo che oramai, data la rilevanza di questi fenomeni e la necessità di realizzare una seria lotta a tali condotte, la scelta del legislatore di inserire le fattispecie secondo una logica di "gemmazione", collocandole a latere di disposizioni già esistenti sulla base del criterio del bene giuridico tutelato, ha determinato un quadro regolatorio troppo frammentato e discontinuo, anche per le continue modifiche imposte dal progresso tecnologico.

Il legislatore dovrebbe perciò utilizzare questo momento per una sistematizzazione delle fattispecie in oggetto evitando di limitarsi a un maquillage del testo codicistico.

La *seconda* considerazione generale riguarda il fatto che sul versante della "resilienza" ci sono una serie di norme di difficile attuazione pratica dovuta a una mancanza di capacità amministrativa e di risorse sia nel breve periodo (nonostante il PNRR) sia (soprattutto) nel lungo periodo.

Il tema è stato ricordato già in altre audizioni. Comprendo che il problema principale per il decisore politico sia dove investire e come spendere in modo efficiente il denaro pubblico ma non dobbiamo dimenticare che nessuna norma, neanche quelle penali, sono a costo zero.

Nel caso di specie, l'introduzione di un "responsabile" o "referente" per la cybersicurezza negli enti indicati all'art. 1 dimostra una notevole attenzione alle nuove sfide presentate dalla cybersicurezza. Peccato però che la semplice presenza di figure di riferimento, peraltro in assenza di una chiara definizione del loro livello di inquadramento, non appare sufficiente a garantire i risultati sperati.

5. Agenzia per la Cybersicurezza Nazionale 2022.
6. Pietropaoli 2023.

È fondamentale che il legislatore, oltre a introdurre novità normative in merito, indichi all'Agenzia per la cybersicurezza nazionale (ACN) di lavorare a stretto contatto con le nuove figure di responsabile o referente che saranno presenti nelle varie amministrazioni, per garantire che i compiti pianificati siano effettivamente realizzati e che vi sia un chiaro processo di monitoraggio e valutazione dei risultati ottenuti, affiancandoli nell'implementazione di strategie operative e di procedure. In coerenza con l'obiettivo garantire un livello elevato di cybersicurezza, vista la natura trasversale e pervasiva della stessa rispetto alla ormai totalità dei servizi di funzionamento delle amministrazioni[7], ai processi digitalizzati e ai servizi erogati verso soggetti terzi, sarebbe opportuno adottare misure in grado di incidere efficacemente e tempestivamente, ad esempio prevedendo che il responsabile o referente per la cybersicurezza esprima pareri sugli atti dell'ente incidenti sulle sue aree di competenza e possa pure emanare linee guida e raccomandazioni interne.

Inoltre, se il disegno di legge pone maggiormente l'accento sulla risposta e l'apparato sanzionatorio in caso di attacchi e minacce informatiche, è altresì importante rivolgere l'attenzione alla prevenzione di tali attacchi, con miglioramenti non solo delle regole giuridiche ma anche con un impegno costante nella formazione e aggiornamento delle competenze di tutto il personale della pubblica amministrazione.

La *terza* considerazione attiene allo scenario che si apre di fronte a noi sul piano normativo nei prossimi mesi[8]. Questo disegno di legge anticipa ma dovrà necessariamente coordinarsi con le norme che verranno approvate dal Governo con decreto legislativo per il recepimento della NIS 2. Penso che immaginarsi il contenuto del disegno di legge oggi in discussione senza avere chiaro o aver esplicitato cosa accadrà su quel fronte sia non corretto. Offro sul punto due considerazioni tecniche. La NIS 2 realizza su tanti fronti un cambiamento di prospettiva rispetto al passato, sia nei termini dei soggetti sia nei termini degli strumenti[9].

Una delle chiavi dell'intervento europeo diviene oggi il sistema di "certificazioni" per la cybersicurezza sul quale siamo chiamati a fare un passo avanti nei prossimi anni. Non è un caso che proprio sul punto è in atto una revisione del Regolamento denominato "EU Cybersecurity Act". Scrivere queste regole senza avere chiaro come si risolverà dall'altra parte il meccanismo certificatorio non aiuta.

L'altra considerazione tecnica mi riporta indietro alla deterrenza penale. Le norme del disegno di legge sul punto andrebbero completate con le regole sul c.d. *ethical hacking* e le forme di garanzia di soggetti che già oggi sono essenziali per la filiera della prevenzione dei reati informatici. La NIS 2 cerca infatti di incoraggiare pratiche coordinate di *vulnerability disclosure*, invitando sia figure esperte sia *ethical hackers* a segnalare le vulnerabilità di prodotti e sistemi, in modo da consentire di diagnosticarle e porvi rimedio prima che vengano divulgate e abusate da terzi. A tal fine l'ENISA sarebbe tenuta a sviluppare e mantenere un registro europeo delle vulnerabilità per consentire ai settori essenziali e importanti, nonché ai loro fornitori di reti e sistemi informativi, di registrare e divulgare le vulnerabilità nei prodotti o nei servizi ICT.

4. Commenti puntuali

Nel tempo che rimane vorrei provare a offrire alla vostra discussione tre commenti più puntuali relative al settore locale e regionale interessato dal Capo I del disegno di legge odierno.

Il *primo* commento riguarda la filosofia di fondo di questi interventi. La cybersicurezza si genera grazie a processi e non solo per adempimenti. La garanzia della resilienza dei sistemi non avviene semplicemente imponendo un onere di notifica e la individuazione di un responsabile unico per ente sul punto. La prima cosa che occorrerebbe capire è quale livello di "maturità della cybersicurezza" hanno gli enti ai quali tali disposizioni si riferiscono. La filosofia dell'intervento legislativo dovrebbe garantire l'aumento dei livelli di consapevolezza e un più pronto riconoscimento dei fattori di rischio, permettendo uno sviluppo proattivo e preventivo della sicurezza informatica.

7. Ursi 2023.
8. Calzolaio-Iannuzzi-Longo et al. 2024, p. 203 ss.
9. Schmitz-Berndt 2023.

Mi immagino perciò che si debba aggiungere una norma che vada concretamente a chiedere alle amministrazioni di essere più consapevoli dei fattori di rischio. Per intenderne l'importanza e comprendere come scriverla, si può vedere cosa prevede il Regolamento (UE, Euratom) 2023/2048 che stabilisce misure per un livello comune elevato di cybersicurezza nelle istituzioni dell'Unione. Per garantire la segnalazione e la notifica occorrono "misure di valutazione e gestione" dei rischi definite anche in "piani per la cybersicurezza". Gli enti menzionati nell'articolo 1 del disegno di legge, perciò, devono essere prima di tutto obbligati ad attivare misure di rilevamento e gestione dei rischi e, nel caso di violazione di legge, dovranno essere sanzionati anche per questo (oltre che per gli eventuali incidenti).

Qualcuno potrebbe farmi notare che si tratta della parte di attuazione della NIS 2, ma allora occorrerebbe precisare anche nel presente disegno di legge che le norme rivolte a rafforzare la cybersicurezza nazionale avranno un necessario completamento nella fase di recepimento della direttiva. Altrimenti, per il tenore delle disposizioni oggi al vostro esame tali obblighi rischiano di rimanere lettera morta o, peggio, di paralizzare i decisori, tanto a livello locale in fase di adempimento quanto a livello nazionale in sede di verifica dell'adempimento stesso.

Il *secondo* commento riguarda il fatto che la cybersicurezza – per usare un'espressione gergale – "si genera insieme" attraverso un quadro conoscitivo chiaro. Nel disegno di legge è dato per scontato che per risolvere i possibili incidenti e garantire la resilienza occorrono soggetti e formule che realizzino una risposta coordinata. È quanto emerge sia nella NIS 2 con riguardo all'EU-CyCLONe e il NIS Cooperation Group sia con riguardo all'emanando regolamento "EU Cybersolidarity Act" che introduce un meccanismo denominato "European Cybersecurity Alert System".

Per questo credo che le norme oggi al vostro esame siano mancanti di un riferimento necessario sia a un meccanismo che per l'Italia si occupi di coordinare la risposta agli incidenti sia della creazione obbligatoria di strutture decentrate che in alcune regioni oggi sono già presenti o stanno per essere attivate di risposta coordinata agli incidenti. Parlo chiaramente dei SOC e della rete nazionale degli CSIRT creati sulla base delle linee guida ACN, i quali realizzano collaborazioni con lo CSIRT Italia per la preparazione e il supporto alla gestione e risposta a incidenti informatici.

Se davvero si vuole imporre agli enti locali e regionali vincoli in materia di cybersicurezza, occorre aiutarli a realizzare effettivamente la resilienza cibernetica indicando una strada concreta per realizzare tale obiettivo. Il modello CSIRT è l'ambito privilegiato sia per identificare i problemi e poi offrire una risposta coordinata agli incidenti informatici sia per realizzare uno scambio di buone pratiche e incentivare il rispetto delle norme.

In tale senso, credo che il referente per la cybersicurezza debba essere in contatto con i costituiti o costituendi CSIRT costituiti nella propria regione, i quali, anche avvalendosi delle in-house regionali e comunali, dovranno vigilare e riportare immediatamente all'ACN ogni incidente, come pure creare un ecosistema innovativo in rete che generi nuova conoscenza sui problemi e le soluzioni (con apertura e contaminazione tra pubblici e privato).

Anche qui potreste ricordarmi che tali norme rientrano nell'attuazione della NIS 2, ma ribadisco che allora ci vuole un coordinamento tra le norme attuali e le emanande disposizioni del decreto legislativo di attuazione.

Il *terzo* e ultimo commento attiene alla realizzazione amministrativa delle esigenze poste dai soggetti che devono gestire a livello locale la cybersicurezza. Stiamo andando incontro a una stagione nella quale sarà molto difficile, soprattutto per via dell'impiego massiccio delle IA, realizzare una efficace resilienza cyber. Gli attacchi oggi sono divenuti più numerosi e più sofisticati.

A questo proposito, propongo di trovare la via per introdurre nell'art. 10 del disegno di legge un riferimento all'art. 75 del nuovo codice dei contratti, d.lgs. n. 36/2023, attraverso l'incentivo di forme di "Partenariato per l'innovazione". Dobbiamo immaginare che, per dotarsi di servizi informatici all'avanguardia, i soggetti pubblici – soprattutto di grandi dimensioni – dovranno non solo rivolgersi al mercato dei servizi già esistenti e consolidati ma anche approvvigionarsi di servizi innovativi da costruire insieme e in coordinamento con aziende operanti in tale settore. In questo senso, il

partenariato per l'innovazione – come è già sostenuto dalla dottrina[10] – potrebbe essere tanto una soluzione da incentivare quanto un possibile volano di crescita economica per tante piccole e medie imprese, come ad esempio quelle nate a partire da *spin-off* universitari.

Riferimenti bibliografici

Agenzia per la Cybersicurezza Nazionale (2022), *Strategia Nazionale di Cybersicurezza 2022-2026*, 2022

R. Brighi (2017), *La vulnerabilità nel cyberspazio*, in "Ars interpretandi", 2017, n. 1

S. Calzolaio, A. Iannuzzi, E. Longo et al. (2024), *La regolazione europea della società digitale*, Giappichelli, 2024

Clusit (2024), *Rapporto 2024 sulla sicurezza ICT in Italia*, 2024

B. Gianmarco, B. Josefa, C. Stephane et al. (2020), *Cybersecurity, our digital anchor (EUR 30276 EN)*, Publications Office of the European Union, 2020

S. Pietropaoli (2023), *Informatica criminale: diritto e sicurezza nell'era digitale*, Giappichelli, 2023

S. Rossa (2023), *Cybersicurezza e Pubblica Amministrazione*, Editoriale Scientifica, 2023

S. Schmitz-Berndt (2023), *Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive,* in "Journal of Cybersecurity", vol. 9, 2023, n. 1

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

R. Ursi (2023), *La sicurezza cibernetica come funzione pubblica*, in Id. (a cura di), "La sicurezza nel cyberspazio", FrancoAngeli, 2023

10. Rossa 2023, p. 169 ss.

Studi e ricerche

Note e discussioni

Osservatori

***Ri*Leggiamoli**

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0156 • articolo sottoposto a peer review • pubblicato in anteprima il 6 giu. 2024

Enrico Albanesi

Le *Linee-guida* dell'Agcom sugli *influencer* nella prospettiva dell'attività di informazione e del costituzionalismo digitale

L'articolo svolge un'analisi critica della regolamentazione degli *influencer* quali fornitori di servizi di media audiovisivi di cui al Testo unico dei servizi di media audiovisivi (TUSMA), compiuta dall'Autorità per le garanzie nelle comunicazioni (Agcom) nelle *Linee-guida* del 2024. Per poter svolgere una siffatta analisi, nell'articolo ci si muove in una prospettiva di diritto costituzionale: accogliendosi, da un lato, la chiave di lettura teorica del costituzionalismo digitale; guardandosi, dall'altro, all'attività degli *influencer* nell'ottica dell'attività di informazione e della libertà di espressione di cui all'art. 21 Cost.

Influencer – Linee-guida Agcom – Fornitore di servizi di media audiovisivi
Fornitore di piattaforma di condivisione di video – Piattaforma online

Agcom Guidelines for vloggers from the perspective of freedom of information and digital constitutionalism

The article is a critical analysis of the 2024 Guidelines, issued by the Italian Communications Regulatory Authority (Agcom), concerning vloggers, in the light of the Italian Audiovisual Media Services Code (TUSMA). The analysis is carried out from a perspective of constitutional law: examining the activities of the vloggers against the 'digital constitutionalism' background and analysing them in light of the legal concept of information and freedom of expression under Article 21 of the Italian Constitution.

vloggers – Agcom guidelines – Audiovisual media service provider – Video-sharing platform provider
Online platform

L'Autore è professore associato di Diritto costituzionale presso il Dipartimento di giurisprudenza dell'Università di Genova

Sommario: 1. Le *Linee-guida* dell'Agcom sugli *influencer*. – 2. L'ambiente digitale, il costituzionalismo digitale e la coregolamentazione. – 3. Le *Linee-guida* dell'Agcom e la riconduzione della categoria degli *influencer* alla fattispecie astratta del «fornitore di servizi di media audiovisivi» di cui all'art. 3, comma 1, lett. *d*), TUSMA. – 4. L'attività degli *influencer*, nella prospettiva della natura dell'attività di informazione e della libertà di espressione di cui all'art. 21 Cost. – 5. Conclusioni. Il costituzionalismo digitale, gli *influencer* ed il più coerente ed efficace strumento di (sia pure indiretto) intervento, costituito dalla regolamentazione delle piattaforme online che ospitano l'attività dei primi.

1. Le *Linee-guida* dell'Agcom sugli *influencer*

Il 10 gennaio 2024 l'Autorità per le garanzie nelle comunicazioni (Agcom) ha approvato le *Linee-guida volte a garantire il rispetto delle disposizioni del Testo unico da parte degli influencer e istituzione di un apposito tavolo tecnico*[1]. La delibera dell'Agcom è giunta all'approvazione a seguito di una consultazione pubblica indetta nel luglio 2023[2].

Secondo la definizione contenuta nel *Report dello European Regulations Group of Audiovisual Media Services* (ERGA) del dicembre 2023, le attività degli *influencer* (anzi: il Report li definisce *vlogger* o *vlogger channel*) hanno in comune il fatto di consistere in «audiovisual content, mostly user-generated, which is uploaded on video sharing platforms and – depending on the type of platforms – is often organized and distributed via channels»[3]. Tali contenuti si caratterizzano per essere *on-demand* ma in alcuni casi anche lineari (*live streams*).

Le *Linee-guida* dell'Agcom (sulla scorta delle conclusioni contenute nel *Report* dell'ERGA) qualificano gli *influencer* come «soggetti che svolgono un'attività analoga o comunque assimilabile» a quella dei fornitori di servizi di media audiovisivi (di cui all'art. 3, comma 1, lett. *d*), "Testo unico dei servizi di media audiovisivi" (TUSMA)), scelta che comporta l'applicabilità ad essi di una serie di disposizioni contenute nello stesso TUSMA[4] (peraltro individuate dalla stessa Agcom nelle *Linee-guida*) che si andranno qui ad esaminare. Scopo del presente articolo è analizzare criticamente tali *Linee guida*.

È bene precisare che le *Linee-guida* sono propedeutiche all'istituzione di un Tavolo tecnico[5] con

1. Cfr. Autorità per le garanzie nelle comunicazioni, *Delibera n. 7/24* – Allegato A.
2. Le principali posizioni emerse nel corso della consultazione pubblica sono reperibili in Autorità per le garanzie nelle comunicazioni, *Delibera n. 7/24*, p. 4 ss.
3. Cfr. European Regulations Group for Audiovisual Media Service. Subgroup 1, *Report – Learning from the practical experiences of NRAs in the regulation of vloggers (Deliverable 3)*, p. 2.
4. Cfr. d.lgs. 8 novembre 2021, n. 208, *Attuazione della direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri, concernente il testo unico per la fornitura di servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato* (come modificato dal d.lgs. 25 marzo 2024, n. 50, *Disposizioni integrative e correttive del decreto legislativo 8 novembre 2021, n. 208, recante il testo unico dei servizi di media audiovisivi in considerazione delle realtà del mercato, in attuazione della direttiva (UE) 2018/1808 di modifica della direttiva 2010/13)*.
5. Cfr. Autorità per le garanzie nelle comunicazioni, *Delibera n. 7/24* – Allegato B.

cui individuare attraverso uno o più codici di condotta le ulteriori misure e le modalità mediante le quali gli *influencer* adeguino la propria attività al fine di garantire il rispetto delle disposizioni del TUSMA (un'operazione "paideutica", verrebbe da dire). Insomma, con le *Linee-guida*, ora, e con il codice di condotta, un domani, ci si sta muovendo nell'ambito della *soft law* al fine (come chiarisce il titolo delle *Linee-guida*) di «garantire il rispetto delle disposizioni del testo unico da parte degli *influencer*».

Le ipotesi di ricerca sono le seguenti.

In primo luogo, si tenterà di dimostrare che la riconduzione della categoria degli *influencer* (sia pure attraverso un'interpretazione analogica) alla fattispecie astratta dei fornitori di media audiovisivi appare in linea tendenziale corretta ma non è sufficientemente circoscritta nelle *Linee-guida*, secondo le invece ben più attente indicazioni contenute nel *Report* dell'ERGA; e che tale riconduzione, così come prospettata nelle *Linee-guida*, va a porre in capo agli *influencer* alcuni «adempimenti e oneri non necessari» che l'Agcom stessa afferma di voler evitare[6]. Forse la strada migliore per regolamentare il fenomeno degli *influencer* sarebbe quella di lasciare tale compito al legislatore, che meglio potrebbe congegnare una più adeguata fattispecie astratta.

In secondo luogo, si proverà a dimostrare che nell'ottica del costituzionalismo digitale (che qui si assumerà come chiave di lettura teorica dell'indagine) la regolamentazione delle piattaforme online che ospitano l'attività degli *influencer* sembra costituire comunque un più coerente ed efficace strumento di intervento, sia pure indiretto, rispetto alla strada percorsa dall'Agcom.

Per poter dimostrare le ipotesi di ricerca, ci si muoverà qui in una prospettiva di diritto costituzionale. Da un lato, definendosi il contesto in cui si svolgono le condotte degli *influencer*: un ambiente digitale, cioè caratterizzato dalla presenza di piattaforme online globali (accogliendosi peraltro qui la chiave di lettura teorica del costituzionalismo digitale) (*infra*, paragrafo 2). Dall'altro lato, dopo aver analizzato le *Linee-guida* (*infra*, paragrafo 3), si esaminerà nel dettaglio la disciplina del TUSMA che le *Linee-guida* individuano come applicabile agli *influencer*, in virtù della qualificazione di questi ultimi come fornitori di servizi di media audiovisivi (*infra*, paragrafo 4). E si guarderà quindi all'attività degli *influencer* nell'ottica dell'attività di informazione e della libertà di espressione di cui all'art. 21 Cost., cercando di dimostrare la prima ipotesi di ricerca che si è prospettata (*infra*, paragrafo 4).

Per concludersi dimostrando la seconda ipotesi di ricerca, nel senso che nell'ottica del costituzionalismo digitale, la regolamentazione delle piattaforme online che ospitano l'attività degli *influencer* sembra costituire un più coerente ed efficace strumento di intervento, sia pure indiretto (*infra*, paragrafo 5).

2. L'ambiente digitale, il costituzionalismo digitale e la coregolamentazione

Gli *influencer* svolgono le loro condotte sulla Rete. Anzi, per essere più precisi, su piattaforme online o piattaforme di condivisione di video.

Nel contesto del Web 2.0[7], le piattaforme online hanno assunto una fisionomia sempre meno passiva e neutrale rispetto ai contenuti veicolati attraverso di esse. Si è altresì passati da una decentralizzazione quasi atomistica degli attori operanti sulla Rete ad una forte centralizzazione in capo a poche piattaforme online globali. A fronte di tale fenomeno, si è dunque iniziato a guardare alla *governance* della Rete in modo differente rispetto a quanto si era soliti fare precedentemente[8]. Si è dunque abbandonata una connotazione eminentemente pubblicistica della libertà di espressione, per accogliersene una di natura anche privatistica. La dimensione digitale vede infatti ormai protagoniste

6. Cfr. Autorità per le garanzie nelle comunicazioni, *Delibera n. 7/24* – Allegato A, p. 3.
7. «Web 2.0 is the network as platform, spanning all connected devices; Web 2.0 applications are those that make the most of the intrinsic advantages of that platform: delivering software as a continually-updated service that gets better the more people use it, consuming and remixing data from multiple sources, including individual users, while providing their own data and services in a form that allows remixing by others, creating network effects through an "architecture of participation," and going beyond the page metaphor of Web 1.0 to deliver rich user experiences». Così O'Reilly 2005. Nella dottrina italiana, cfr. Orofino 2008, p. 13 ss.
8. Cfr. Cerf 2022 e Scorza 2022, rispettivamente p. 17 ss. e p. 23 ss.

le piattaforme online: «spazi formalmente privati», come si è notato, «che, però, sono entrati prepotentemente a far parte della sfera pubblica»[9]. Detto altrimenti, con l'avvento delle piattaforme online globali, la libertà di espressione in Rete non si svolge più nella tradizionale dimensione verticale (Stato/cittadino) ma in una dimensione triangolare, in cui il nuovo attore è costituito da soggetti privati (le piattaforme online) che, come si è detto, non svolgono più un ruolo meramente neutrale rispetto al contenuto veicolato in Rete, anche solo per l'organizzazione dello stesso[10].

È in questo contesto che si è sviluppata la prospettiva teorica del costituzionalismo digitale, inteso come "ideologia" volta a porre limiti ai poteri privati sulla Rete (ormai entrati però a far parte della sfera pubblica), così come a partire dal Diciottesimo secolo il costituzionalismo è volto, nel mondo "reale", a limitare (specie ma non solo) i poteri pubblici[11]. La necessità sottesa a tale approccio teorico è quella di contemperare la libertà di manifestazione del pensiero, che si esplica in Rete, con la tutela del valore della dignità umana, la tutela di specifici diritti altrui, il contrasto alla diffusione di discorsi d'istigazione alla violenza o all'odio nonché di contenuti in violazione del diritto d'autore o nocivi per i minori.

Tale contemperamento è stato peraltro compiuto dalla giurisprudenza delle Corti europee (la Corte di giustizia dell'Unione europea e la Corte europea dei diritti dell'uomo) nei primi anni dell'avvento di tali piattaforme[12]. Tuttavia, a livello europeo è solo il *legislatore* (dunque, il legislatore dell'Unione europea) che poteva intervenire ad introdurre nuove forme di "regolamentazione" giuridica e tecnica delle piattaforme online, nell'ottica del costituzionalismo digitale sopra menzionato. Forme di "regolamentazione" che non solo consentissero l'accertamento della responsabilità dei soggetti che caricano contenuti illeciti veicolati in Rete (responsabilità che permane, ovviamente[13]); ma anche impedissero o ponessero fine ad illeciti e consentissero che la pubblica autorità sia informata degli illeciti e riceva informazioni richieste.

Nel dibattito su quale sia il "livello" più adeguato di siffatte forme di "regolamentazione" e nelle esperienze pratiche, è stata contemplata una pluralità di soluzioni. Nei primi anni in cui tali problematiche si sono manifestate e si è cercato di dare ad esse risposta, si erano affermate "carte di diritti"[14] ed esperienze di autoregolamentazione che, da sole, non hanno però funzionato al meglio[15]. L'Unione europea ha però di recente individuato la strada della coregolamentazione, con l'introduzione dunque di obblighi tecnico-organizzativi in capo alle piattaforme online, al fine di attribuire a queste ultime il compito di moderazione dei contenuti da pubblicarsi attraverso esse.

Va detto peraltro come non ci sia in realtà accordo in dottrina sulla riconduzione alla categoria della autoregolamentazione o della coregolamentazione[16] delle fattispecie introdotte dall'Unione europea in tale campo. Alcuni autori le considerano autoregolamentazione, in quanto il compito di effettuare l'attività di moderazione dei contenuti è comunque rimessa alle piattaforme online[17]. Il fatto però che alla luce delle recenti normative dell'Unione europea si sia realizzato un «collegamento giuridico tra l'autoregolamentazione

9. Così Bassini 2019, p. 15 nonché p. 108 ss. Cfr. anche Pollicino-De Gregorio 2021, p. 6.
10. Cfr. Balkin 2018, p. 2011 ss.
11. Cfr. per tutti De Gregorio 2022, p. 4 ss. e Pollicino 2021, p. 2.
12. Cfr. Orofino 2014, p. 35 ss.
13. Cfr. Bassini 2019, p. 111.
14. Cfr. Celeste 2023.
15. In senso critico sull'autoregolamentazione, cfr. Pollicino-De Gregorio 2021, p. 12 e Crawford 2021, p. 256. Secondo Bassini 2019, p. 106, le carte dei diritti hanno rappresentato un cambio di paradigma ma difficilmente possono costituire di per sé una soluzione.
16. Su cui cfr. le definizioni contenute, ad esempio, nel *Parere del Comitato economico e sociale europeo sul tema «Autoregolamentazione e coregolamentazione nel quadro legislativo dell'UE»*, 2015/C 2019/05. Sulla *soft law* nell'Unione europea, cfr. De Witte 2023, p. 101 ss.
17. Cfr. Niro 2021, p. 1390.

e il legislatore», novità rispetto ai tempi in cui la regolamentazione era rimessa alla «iniziativa volontaria» (elemento che caratterizza la autoregolamentazione) delle piattaforme private, sembra condurre altri Autori[18] a meglio qualificare tali fattispecie in termini di coregolamentazione[19].

In ogni modo, al di là della riconduzione all'una o all'altra fattispecie e venendosi al contenuto di tali discipline di derivazione europea, è stata approvata una disciplina di carattere generale dei prestatori di servizi intermediari e, segnatamente, dei prestatori di servizi di memorizzazione di informazioni (comprese le piattaforme online) nel *regolamento sui servizi digitali* (2022)[20]; una disciplina dei fornitori di piattaforma per la condivisione video nella nuova direttiva sui servizi di media audiovisivi (2018)[21]; una disciplina dei servizi di condivisione online nella direttiva sul diritto d'autore nel mercato unico digitale (2019)[22]. Questi ultimi due atti sono stati recepiti dall'Italia, rispettivamente con il d.lgs. recante il TUSMA (2021)[23] e con il d.lgs. in materia di diritto d'autore nel mercato unico digitale (2021)[24].

Come si accennava, ciò che caratterizza tali discipline è l'introduzione di una serie di obblighi tecnico-organizzativi (sostanzialmente: di moderazione dei contenuti) in capo ai prestatori di servizi di intermediazione, segnatamente le piattaforme online[25]. Un intervento, questo, non certo "indolore" dal punto di vista costituzionale.

In primo luogo, occorre infatti segnalare la potenziale restrizione della libertà di manifestazione del pensiero derivante dall'imposizione di obblighi tecnico-organizzativi in capo ai prestatori di servizi di intermediazione (questione che però la Corte di giustizia dell'Unione europea ha risolto

18. Parlano delle recenti normative introdotte dall'Unione europea come «alternativa al modello di *self-regulation*» e come mezzo per «limitare drasticamente l'autoregolamentazione», rispettivamente, Santaniello 2022, p. 68 e Caggiano 2021, p. 13.
19. Cfr. il *Considerando 14* della nuova *direttiva sui servizi di media audiovisivi* (citata, *infra*, in nota 21): «La coregolamentazione, nella sua forma minima, fornisce un collegamento giuridico tra l'autoregolamentazione e il legislatore nazionale, in conformità con le tradizioni giuridiche degli Stati membri. Nella coregolamentazione le parti interessate e il governo o l'autorità o gli organismi nazionali di regolamentazione condividono il ruolo di regolamentazione. Il ruolo delle autorità pubbliche competenti comprende il riconoscimento del regime di coregolamentazione, l'audit dei suoi processi e il suo finanziamento. La coregolamentazione dovrebbe consentire l'intervento statale qualora i suoi obiettivi non siano conseguiti». Dal canto suo, l'«autoregolamentazione costituisce un tipo di iniziativa volontaria che permette agli operatori economici, alle parti sociali, alle organizzazioni non governative e alle associazioni di adottare fra di loro e per se stessi orientamenti comuni. Spetta a loro sviluppare, monitorare e garantire il rispetto di tali orientamenti. [Essa costituisce] uno strumento complementare per attuare determinate disposizioni della direttiva [ma] non dovrebbe sostituirsi ai compliti del legislatore nazionale».
20. Cfr. 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)*.
21. Cfr. direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio 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*.
22. Cfr. direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio 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*.
23. Cfr. d.lgs. 8 novembre 2021, n. 208, cit.
24. Cfr. d.lgs. 8 novembre 2021, n. 177, *Attuazione della direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, 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*.
25. Su tali discipline, nell'ottica del costituzionalismo digitale di cui si è dato qui conto, sia consentito il rinvio a Albanesi-Valastro-Zaccaria 2023, p. 189 ss.

negativamente, quantomeno con riguardo ad un caso specifico nel 2019[26]). Dall'altro, stanno i rischi derivanti dalla censura privata svolta da soggetti (le piattaforme online) cui è attribuito il compito di moderazione dei contenuti[27].

Si vedrà in sede di *Conclusioni* come nella prospettiva del costituzionalismo digitale, qui richiamata, la regolamentazione delle piattaforme online che ospitano l'attività degli *influencer* potrebbe costituire un più coerente ed efficace strumento di intervento, sia pure indiretto, rispetto alla strada percorsa dall'Agcom.

3. Le *Linee-guida* dell'Agcom e la riconduzione della categoria degli *influencer* alla fattispecie astratta del «fornitore di servizi di media audiovisivi» di cui all'art. 3, comma 1, lett. *d*), TUSMA

È però ora indispensabile analizzare il contenuto delle *Linee-guida*.

L'Agcom individua l'obiettivo delle *Linee guida* nell'esigenza di individuare: le disposizioni del TUSMA che gli *influencer* sono tenuti a rispettare e le misure necessarie a garantirne l'uniforme e coerente applicazione, con particolare riferimento, al rispetto dei principi di trasparenza e della correttezza dell'informazione, all'applicazione della disciplina in materia di tutela dei minori e dei diritti fondamentali della persona ed alle disposizioni in materia di comunicazioni commerciali e di *product placement* volte a rendere trasparenti al pubblico le finalità promozionali eventualmente perseguite[28].

Per raggiungere tale obiettivo, l'Agcom riconduce l'attività dell'*influencer* alla disciplina legislativa disposta per il «fornitore di servizi di media audiovisivi» di cui all'art. 3, comma 1, lett. *d*), TUSMA, cioè «la persona fisica o giuridica cui è riconducibile la responsabilità editoriale della scelta del contenuto audiovisivo o radiofonico del servizio di media audiovisivo o radiofonico e che ne determina le modalità di organizzazione». Per «servizio di media audiovisivo» si intende un servizio il cui obiettivo principale sia la fornitura di programmi al grande pubblico al fine di informare, intrattenere o istruire (art. 3, comma 1, lett. *a*), TUSMA).

Tuttavia, alla luce delle *Linee-guida*, non tutti gli *influencer* sono qualificabili come fornitore di servizi di media audiovisivi ma solo quelli che rispondono a determinati criteri. Questa è una scelta che l'Agcom compie in conformità con le raccomandazioni del *Report* dell'ERGA, dove si legge che «[g]uidelines should elaborate how the different criteria of the definition of AVMS can be understood and applied in the situation of vloggers»[29]. In particolare, i criteri che l'ERGA individua sono lo svolgimento di un «economic service», il fatto che «the principal purpose should be to inform, entertain, or educate the general public» nonché l'accessibilità del servizio al «general public»[30].

Questo approccio si riscontra anche nelle *Linee-guida* dell'Agcom, financo nel linguaggio usato. A rigore, l'Agcom non qualifica infatti gli *influencer* direttamente come fornitori di servizi di media audiovisivi. Nelle *Linee-guida* l'Agcom nota come gli *influencer* sono quei soggetti che svolgono «un'attività *analoga* o *comunque assimilabile* a quella dei fornitori di servizi di media audiovisivi» (corsivi aggiunti)[31]. Anche nella delibera stessa, quando sono rappresentate le principali posizioni emerse nella consultazione pubblica, l'Agcom nota come gli *influencer* «si collocano tra il fornitore di servizi [di] media […] e un *quisque de populo* che esprime liberamente il proprio pensiero in rete senza alcun intento economico»[32].

26. Cfr. Corte di giustizia (Grande sezione), sentenza 26 aprile 2022, C-401/19, *Polonia c. Parlamento europeo e Consiglio dell'Unione europea*, paragrafo 39 ss.
27. Sugli Stati Uniti, cfr. Balkin 1999, p. 2295 ss. In Italia, cfr. Grandinetti 2022, specie p. 241 ss., Bassini 2019, p. 111 e Monti 2019.
28. Cfr. Autorità per le garanzie nelle comunicazioni, *Delibera n. 7/24* – Allegato A, p. 2.
29. Cfr. European Regulations Group for Audiovisual Media Service. Subgroup 1, *Report*, cit., p. 16.
30. *Ivi*, p. 3 ss.
31. Cfr. Autorità per le garanzie nelle comunicazioni, *Delibera n. 7/24* – Allegato A, p. 1.
32. Cfr. Autorità per le garanzie nelle comunicazioni, *Delibera n. 7/24*, p. 4 ss.

Le *Linee-guida* individuano quindi una serie di caratteristiche che i soggetti devono possedere cumulativamente per essere qualificati come *influencer*. Si tratta delle seguenti: *a*) il servizio offerto costituisce attività economica ai sensi degli articoli 56 e 57 TFUE; *b*) lo scopo principale del servizio offerto è la fornitura di contenuti, creati o selezionati dall'*influencer*, che informano, intrattengono o istruiscono e che sono suscettibili di generare reddito direttamente in esecuzione di accordi commerciali o indirettamente in applicazione degli accordi di monetizzazione applicati dalla piattaforma o dal *social media* utilizzato; *c*) l'*influencer* ha la responsabilità editoriale sui contenuti, la quale include il controllo effettivo sulla creazione, sulla selezione o sulla organizzazione dei contenuti medesimi; *d*) il servizio è accessibile al grande pubblico, raggiunge un numero significativo di utenti sul territorio italiano, ha un impatto rilevante su una porzione significativa di pubblico e i contenuti sono diffusi tramite un servizio di piattaforma di condivisione video o di *social media*; *e*) il servizio consente la fruizione dei contenuti su richiesta dell'utente; *f*) il servizio è caratterizzato da un legame stabile ed effettivo con l'economia italiana; *g*) i contenuti sono offerti tramite l'utilizzo della lingua italiana[33].

L'Agcom precisa però che le disposizioni dell'EMFA si applicano solo agli «*influencer* che svolgono attività professionale», escludendosi dunque i soggetti che operano in maniera meno continuativa e strutturata (cioè, quelli che svolgono mera attività amatoriale). I primi (cioè quelli a cui si applica la disciplina di cui al TUSMA e che potrebbero definirsi come "sopra soglia") sono, secondo le *Linee-guida*, quegli *influencer* che: *a*) raggiungono un numero di iscritti (i cosiddetti *follower*) pari, in sede di prima applicazione, ad almeno un milione, risultanti dalla somma degli iscritti sulle piattaforme e dei *social media* su cui operano; *b*) hanno pubblicato nell'anno precedente alla rilevazione almeno 24 contenuti aventi le caratteristiche definite dalle presenti *Linee guida*; *c*) abbiano superato almeno su una piattaforma o *social media* un valore di *engagement rate* medio negli ultimi 6 mesi pari o superiore al 2%[34].

Come si è detto, la circoscrizione dell'area di applicabilità della disciplina del TUSMA, ai soli soggetti che presentano queste ultime caratteristiche, è in linea con il *Report* dell'ERGA. Tuttavia, non sembra che le *Linee-guida* dell'Agcom abbiano sufficientemente circoscritto la riconduzione della categoria degli *influencer*, secondo le invece ben più attente indicazioni contenute nel *Report* dell'ERGA.

Si andrà a dimostrare questo assunto, riflettendosi sulla natura dell'attività di informazione.

4. L'attività degli *influencer*, nella prospettiva della natura dell'attività di informazione e della libertà di espressione di cui all'art. 21 Cost.

Seguendosi il ragionamento dell'Agcom, le *Linee-guida* puntualizzano che agli *influencer* "sopra soglia" si applica la seguente disciplina legislativa di cui al TUSMA.

In primo luogo, si tratta dei principi generali di cui all'articolo 4, comma 1, TUSMA (quali il rispetto della dignità umana, il contrasto alle strategie di disinformazione, la tutela dei diritti d'autore, ecc.). Seguono i principi generali cui all'articolo 6, comma 2, lett. *a*), TUSMA, in materia di informazione, in quanto applicabili (si tratta in questo caso della presentazione veritiera dei fatti e degli avvenimenti, in modo da favorire la libera informazione delle opinioni). In terzo luogo, le disposizioni a tutela del diritto d'autore richiamate nell'articolo 32 TUSMA. Poi, le disposizioni a tutela dei diritti fondamentali della persona, dei minori e dei valori dello sport di cui agli articoli 30, 37, 38 e 39 TUSMA e delle pertinenti delibere attuative adottate dall'Autorità. Infine, le disposizioni in materia di comunicazioni commerciali di cui agli articoli 43, 46, 47 e 48 TUSMA[35].

Occorre a questo punto cercare di ragionare sulla natura dell'attività degli *influencer*, nella prospettiva dell'attività di informazione e della libertà di espressione di cui all'art. 21 Cost., per tentare di comprendere se esista davvero una similitudine tra gli *influencer* e i fornitori di servizi di media audiovisivi, tale da giustificare l'estensione analogica, ai primi, della disciplina del TUSMA.

33. Cfr. Autorità per le garanzie nelle comunicazioni, *Delibera n. 7/24* – Allegato A, p. 1 ss.
34. *Ivi*, p. 3.
35. *Ivi*, p. 4.

Quanto all'essenza dell'attività degli *influencer*, le *Linee-guida* sembrano individuarla, come si è già detto, nella «fornitura di contenuti, creati o selezionati dall'*influencer*, che informano, intrattengono o istruiscono e che sono suscettibili di generare reddito direttamente in esecuzione di accordi commerciali o indirettamente in applicazione degli accordi di monetizzazione applicati dalla piattaforma o dal *social media* utilizzato»[36].

Ebbene, prima di rispondere alla domanda circa la effettiva similitudine tra gli *influencer* e i fornitori di servizi di media audiovisivi, appare opportuno chiedersi se non vi fossero altre fattispecie astratte nel TUSMA cui potenzialmente ricondurre l'attività degli *influencer*.

La prima potrebbe essere quella del «video generato dall'utente» di cui all'art. 3, comma 1, lett. *h*), TUSMA. Con riferimento a questa, la risposta sembra negativa, in quanto limitata ad una serie di immagini animate, sonore o non, che costituiscono un singolo elemento. Nel caso dell'*influencer* è chiaro che l'attività si riferisce ad una pluralità di contenuti, creati, selezionati o organizzati da questi.

La seconda fattispecie potrebbe essere quella del «servizio di piattaforma per la condivisione video» di cui all'art. 3, comma 1, lett. *c*), TUSMA. Volendo, si potrebbe affiancare a questa anche una fattispecie esterna al TUSMA: quella di «piattaforma online» di cui all'art. 3, paragrafo 1, lett. *i*), del sopra citato *regolamento sui servizi digitali*. Ebbene, anche in questo caso la risposta sembra essere negativa perché l'*influencer* non si limita a fornire programmi e/o video generati dagli utenti oppure a memorizzare e diffondere informazioni al pubblico: l'*influencer* crea, seleziona o organizza tali contenuti, sia pure caricandoli su piattaforme online o piattaforme di condivisione video.

Torna quindi la domanda di partenza: l'attività degli *influencer* è assimilabile a quella dei fornitori di servizi di media audiovisivi, a tal punto da giustificare l'estensione analogica, ai primi, della disciplina del TUSMA?

La questione può essere vista da due distinte angolazioni.

La prima angolazione è la prospettiva della natura dell'attività di informazione.

Ebbene, l'attività degli *influencer* può qualificarsi come fornitura di programmi al fine di informare, intrattenere o istruire, sotto la responsabilità editoriale del fornitore, come richiede l'art. 3, comma 1, lett. *a*), TUSMA[37]?

Come nota l'ERGA, l'attività degli *influencer* può qualificarsi come *on demand* ma anche, in alcuni casi, lineare (*live streams*). Dunque, anche con riguardo all'attività degli *influencer* possono venire in rilievo «programmi» (come richiede l'art. 3, comma 1, lett. *a*), TUSMA), sebbene nelle *Linee-guida* si parli di generici «contenuti». Ai sensi dell'art. 3, comma 1, lett. *g*), TUSMA, «programmi» sono «una serie di immagini animate, sonore o non, escluse le cosiddette gif, che costituiscono un singolo elemento, indipendentemente dalla sua durata, nell'ambito di un palinsesto o di un catalogo *stabilito* da un fornitore di servizi di media audiovisivi, comprensivo di lungometraggi, videoclip, manifestazioni sportive, commedie di situazione (sitcom), documentari, programmi per bambini e fiction originali». Ai sensi dell'art. 3, comma 1, lett. *n*), TUSMA «palinsesto televisivo» è «l'insieme, predisposto da un'emittente televisiva […] di una serie di programmi unificati da un medesimo marchio editoriale e destinato alla fruizione del pubblico, diverso dalla trasmissione differita dello stesso palinsesto, dalla trasmissioni meramente ripetitive, o dalla prestazione, a pagamento, di singoli programmi, o pacchetti di programmi, audiovisivi lineari […]». Ed ai sensi dell'art. 3, comma 1, lett. *o*), TUSMA, per «responsabilità editoriale» si intende «esercizio di un controllo effettivo sia sulla selezione dei programmi, […] sia sulla loro organizzazione in un palinsesto cronologico, nel caso delle radiodiffusioni televisive o radiofoniche, o in un catalogo, nel caso dei servizi di media audiovisivi a richiesta». *Nulla quaestio* su questi caratteri, per quanto riguarda gli *influencer*.

Il *punctum dolens* è un altro.

Davvero si può giungere a "nobilitare" *tutta* l'attività degli *influencer*, qualificandola sempre in termini di fornitura di contenuti che «informano, intrattengono o istruiscono» ai sensi dell'art. 3, comma 1, lett. *a*), TUSMA? In altri termini, davvero si può attribuire a tutta l'attività degli *influencer* la qualifica di «servizio di interesse generale» (cioè,

36. *Ivi*, p. 1 ss.

37. Sulla nozione di fornitore di servizi di media audiovisivi, cfr. Grandinetti 2021, p. 286 ss.

in altri termini, di servizio pubblico) che la qualifica di «servizio di media audiovisivo» si porterebbe con sé, ai sensi dell'art. 6, comma 1, TUSMA?

L'attività degli *influencer* è di per sé connotata dal fatto di essere «suscettibile di generare reddito direttamente in esecuzioni di accordi commerciali con produttori di beni e servizi o indirettamente in applicazione degli accordi di monetizzazione applicati dalla piattaforma o dal *social media* utilizzato».

Un parallelo viene da farsi con il caso delle c.d. interviste a pagamento (interviste rilasciate da Consiglieri regionali ad emittenti locali dietro corresponsione di somme di denaro da parte degli intervistati a tali emittenti)[38]; oppure con l'utilizzo, all'interno di telegiornali e programmi di informazione, di tecniche quali il videomessaggio o l'intervista dalle caratteristiche anomale [39]. Con riferimento a tali fattispecie, gli organi regolatori, che se ne sono in passato occupati, hanno sempre statuito che la condotta onerosa o il ricorso a determinate tecniche comunicative rendessero impossibile la loro riconduzione alla fattispecie dell'informazione. *Mutatis mutandis*, lo stesso sembra potersi affermare con riferimento all'attività degli *influencer*: la generazione di reddito, nelle forme di cui si è detto, è talmente inscindibile con l'attività degli *influencer* da doversi escludere che questa possa qualificarsi sempre come attività di informazione, intrattenimento o istruzione nei termini di servizio di interesse generale cui fa riferimento il TUSMA.

Non è un caso se nel *Report* dell'ERGA si nota come siano necessari alcuni indicatori quantitativi e/o qualitativi per individuare che lo scopo principale del servizio sia quello di informare, intrattenere o istruire. Nel *Report* si fa riferimento, ad esempio, alla proporzione tra i video che consistano nella mera promozione di prodotti o servizi e gli altri video; alla natura e all'origine del soggetto; a quanto sia chiaramente percepibile l'intento al pubblico l'intento promozionale del canale. L'ERGA ammette che possa essere difficile tracciare una linea di confine ma sottolinea come l'approccio debba essere casistico e come a tal fine vadano individuati dei criteri distintivi.

Ebbene, questi sembrano mancare del tutto nelle *Linee-guida*.

Certo, è vero che già oggi l'art. 47, comma 4, TUSMA (e, a monte di questo, l'art. 25 della direttiva 2010/13/UE a cui il TUSMA dà attuazione) fa riferimento «ai palinsesti dedicati esclusivamente alla pubblicità, alle televendite, ovvero all'autopromozione», implicitamente riconducendo senz'altro, dunque, alla categoria dei fornitori di media audiovisivi quelli dedicati esclusivamente alle televendite. Le riflessioni del *Report* dell'ERGA sulla necessità di indicatori quantitativi e/o qualitativi per individuare che lo scopo principale del servizio sia quello di informare, intrattenere o istruire, dovrebbero forse condurre ad un ripensamento di siffatta riconduzione *tout court* di tali palinsesti alla fattispecie in questione.

La seconda angolazione è quella della libertà di espressione di cui all'art. 21 Cost. (dunque, la prospettiva, questa volta, degli *influencer*).

Come l'Agcom nota nelle *Linee-guida*, agli *influencer* si applicherebbe, tra l'altro, l'art. 6, comma 2, lett. *a*), TUSMA, cioè, come si è detto, l'obbligo di presentazione veritiera dei fatti. Le *Linee-guida* si spingono addirittura oltre, richiedendo che gli *influencer* si impegnano anche a «verificare la correttezza e l'obiettività delle informazioni anche attraverso la menzione delle fonti utilizzate, nonché a porre in essere azioni di contrasto alla disinformazione online nell'ambito delle iniziative proposte dal Tavolo tecnico»[40]. Tutto ciò (l'assenza, cioè, di quei criteri distintivi riguardanti lo scopo principale consistente nell'informare, intrattenere o istruire), sembra però introdurre in capo a (tutti) gli *influencer* proprio quegli «adempimenti e oneri non necessari» che l'Agcom stessa afferma di voler evitare[41].

Non si vuole certo qui negare la necessità di dare una risposta al problema della pubblicità ingannevole né della disinformazione che gli *influencer* potrebbero veicolare. Si vuole solo sottolineare, da un lato, come non *tutta* l'attività svolta dagli

38. Cfr., volendo, Albanesi 2016.

39. Per approfondimenti su tali tecniche, sulla relativa casistica e sugli interventi regolatori o sanzionatori della Commissione di vigilanza RAI e dell'Agcom, sia consentito il rinvio a Albanesi 2012, p. 487 ss.

40. Cfr. Autorità per le garanzie nelle comunicazioni, *Delibera n. 7/24* – Allegato A, p. 5.

41. *Ivi*, p. 3.

influencer sia assimilabile a quella dei fornitori di servizi di media audiovisivi; dall'altro, conseguentemente, come non a *tutti* o comunque non *sempre* possa applicarsi la disciplina in materia di informazione di cui al TUSMA.

5. Conclusioni. Il costituzionalismo digitale, gli *influencer* ed il più coerente ed efficace strumento di (sia pure indiretto) intervento, costituito dalla regolamentazione delle piattaforme online che ospitano l'attività dei primi

In conclusione, viene allora da chiedersi se la strada preferibile per regolamentare il fenomeno degli *influencer* non sia forse piuttosto quella di lasciare tale compito al legislatore, che meglio potrebbe congegnare una più adeguata fattispecie astratta, facendosi carico delle esigenze che in questa sede si è cercato di evidenziare: quella di non ricondurre *tutta* l'attività degli *influencer* alla fattispecie dell'informazione/intrattenimento/istruzione e (conseguentemente) quella di non addossare in capo agli *influencer* adempimenti e oneri non necessari.

Anche a non volersi attendere un intervento del legislatore, nel *Report* dell'ERGA, come si è già notato, si auspica comunque che la riconduzione degli *influencer* alla fattispecie astratta dei fornitori di servizi di media audiovisivi sia circoscritta attraverso indici quantitativi o qualitativi concernenti il servizio di informazione, intrattenimento o istruzione svolto: elemento, questo, che manca nelle *Linee guide* dell'Agcom, nel senso che già si è detto (*supra*, paragrafo 4).

C'è però un'ulteriore e conclusiva notazione che merita di essere svolta nella prospettiva della libertà di espressione, intesa ("alla Balkin") come un triangolo, e del costituzionalismo digitale (*supra*, paragrafo 2), che qui si è accolta.

Non sembra, cioè, che l'Agcom abbia valorizzato a sufficienza discipline legislative parallele, applicabili (forse in modo più coerente ed efficace, sebbene indiretto) alla fattispecie degli *influencer*, se non menzionandole l'Agcom *en passant* nelle *Linee-guida*.

Queste ultime (e, un domani, il *Codice di condotta*) vanno infatti ad incidere sul vertice del triangolo rappresentato dal cittadino (in questo caso: gli *influencer*) e non sul vertice costituito dagli attori privati (le piattaforme online/piattaforme di condivisione video).

Esistono infatti discipline già applicabili indirettamente all'attività degli *influencer* e sono quelle in materia di fornitori di piattaforma per la condivisione di condivisione video (di cui al TUSMA) e, più in generale, in materia di piattaforme online (di cui al *regolamento sui servizi digitali*). Discipline da applicarsi appunto in questo caso alle piattaforme online che ospitano i contenuti creati, selezionati o organizzati dagli *influencer*.

In primo luogo, si tratta della disciplina (che qui più specificamente interessa, dato il fenomeno in esame) in materia di comunicazione commerciale. È il caso dell'art. 43 TUSMA avente ad oggetto comunicazioni commerciali (articolo che, per il tramite dell'art. 42, comma 2, TUSMA, si applica ai fornitori di piattaforma per la condivisione di video); dell'art. 46 TUSMA sulle sponsorizzazioni (articolo applicabile ai fornitori di piattaforma per la condivisione di video ai sensi della definizione di «sponsorizzazione», contenuta nell'art. 3, comma 1, lett. *ss*), TUSMA); nonché dell'art. 48 TUSMA sull'inserimento dei prodotti (articolo applicabile ai fornitori di piattaforma per la condivisione di video ai sensi della definizione di «inserimento dei prodotti», di cui all'art. 3, comma 1, lett. *uu*), TUSMA)[42].

In secondo luogo, è il caso della disciplina in materia di contenuti illegali (es.: contenuti nocivi per i minori o discorsi d'odio) di cui all'art. 42 TUSMA[43] e di cui al *regolamento sui servizi digitali*.

In terzo luogo, trova applicazione in tale ambito la disciplina a tutela del diritto d'autore di cui al d.lgs. in materia di diritto d'autore nel mercato unico digitale.

Attraverso questi atti normativi, come si accennava (*supra*, paragrafo 2), è stata infatti introdotta una serie di obblighi tecnico-organizzativo (sostanzialmente: di moderazione dei contenuti) in capo ai prestatori di servizi di intermediazione,

42. Su tali fattispecie cfr., volendo, Albanesi-Valastro-Zaccaria 2023, p. 324 ss.

43. Sottolineano come l'inclusione dei servizi di piattaforma di condivisione video nella disciplina dei servizi di media audiovisivi abbia avuto come obiettivo quello di ridurre il *gap* tra le discipline delle due categorie Cuniberti-Bassini 2022, p. 374. In particolare, nella prospettiva della tutela dei minori, cfr. anche De Minico 2019 e Donati 2019, p. 99 ss. e p. 125 ss.

segnatamente le piattaforme online e le piattaforme di condivisioni video[44]. Come detto, per quanto rileva in questa sede, tali obblighi di rimozione riguarderebbero quei contenuti creati, selezionati o organizzati dagli *influencer*.

In questo modo si potrebbe fare dunque ricorso a tutto l'apparato regolatorio e sanzionatorio nonché a quelle misure tecnico-organizzative di moderazione dei contenuti in capo alle piattaforme online già in fase avanzata di rodaggio.

Le *Linee-guida* si limitano a menzionare (alcune di) queste discipline.

L'Agcom sottolinea infatti come le disposizioni del TUSMA «coincidono parzialmente con i termini e le condizioni già applicati dalle piattaforme per la condivisione di video e dei social media, con gli obblighi di trasparenza e riconoscibilità delle comunicazioni commerciali e con il quadro normativo in materia di tutela dei consumatori»; e come per i servizi di piattaforma per la condivisione di video continuano ad applicarsi le disposizioni di cui agli artt. 41, 42 e 43 TUSMA in quanto «tali piattaforme rappresentano lo strumento tramite il quale gli *influencer* rendono disponibili al pubblico i propri contenuti»[45].

In conclusione, nell'operazione "paideutica" nei confronti degli *influencer* ad opera delle *Linee-guida*, l'Agcom avrebbe potuto inserire quegli indicatori quantitativi e/o qualitativi raccomandati dall'ERGA per individuare che lo scopo principale del servizio sia quello di informare, intrattenere o istruire. Sebbene, come si è detto, il legislatore potrebbe farlo più adeguatamente del regolatore.

In ogni caso l'Agcom avrebbe forse potuto coinvolgere, in un'azione di coregolamentazione in conformità con i paradigmi del costituzionalismo digitale, il vertice del triangolo costituito dalle piattaforme online e dalle piattaforme di condivisione video, per gestire il fenomeno degli *influencer*.

Riferimenti bibliografici

L. Abba, A. Lazzaroni, M. Pietrangelo (a cura di) (2022), *La Internet governance e le sfide della trasformazione digitale*, Editoriale scientifica, 2022

G.B. Abbamonte, E. Apa, O. Pollicino (a cura di) (2019), *La riforma del mercato audiovisivo europeo*, Giappichelli, 2019

E. Albanesi (2016), *Le "interviste a pagamento" di consiglieri regionali nelle emittenti locali. Tra libertà d'impresa, diritto ad essere informati e pluralismo dell'informazione*, in M. Grondona (a cura di), "Libertà, persona, impresa, territorio. Visioni interdisciplinari a confronto", Aracne, 2016, pp. 191-206

E. Albanesi (2012), *Tecniche comunicative al confine tra informazione e comunicazione politica. Quid iuris?*, in M. Villone, A. Ciancio, G. De Minico et al. (a cura di), "Nuovi mezzi di comunicazione e identità: omologazione o diversità?", Aracne, 2012, pp. 477-497

E. Albanesi, A. Valastro, R. Zaccaria (2023), *Diritto dell'informazione e della comunicazione*, XII ed., Cedam, 2023

J. Balkin (2018), *Free Speech is a Triangle,* in "Columbia Law Review", vol. 118, 2018, n. 7, pp. 2011-2056

J. Balkin (1999), *Free Speech and Hostile Environments*, in "Columbia Law Review", vol. 99, 1999, n. 8, pp. 2295-2320

M. Bassini (2019), *Internet e libertà d'espressione. Prospettive costituzionali e sovranazionali*, Aracne, 2019

G. Caggiano (2021), *La proposta di Digital Service Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in G. Caggiano, G. Contaldi, P. Manzini (a cura di), "Verso una legislazione europea su mercati e servizi digitali", Cacucci editore, 2021, pp. 3-29

44. Per approfondimenti, cfr. volendo Albanesi-Valastro-Zaccaria 2023, p. 204 ss.

45. Cfr. Autorità per le garanzie nelle comunicazioni, *Delibera n. 7/24* – Allegato A, pp. 6-7.

G. Caggiano, G. Contaldi, P. Manzini (a cura di) (2021), *Verso una legislazione europea su mercati e servizi digitali*, Cacucci editore, 2021

V. Cerf (2022), *Sulla governance di Internet*, in L. Abba, A. Lazzaroni, M. Pietrangelo (a cura di), "La Internet governance e le sfide della trasformazione digitale", Editoriale scientifica, 2022, pp. 17-22

E. Celeste (2023), *Digital Constitutionalism. The role of Internet bills of rights*, Routledge, 2023

C. Contessa, P. Del Vecchio (a cura di) (2021), *Testo unico servizi di media audiovisivi*, La Tribuna, 2021

K. Crawford (2021), *Né intelligente né artificiale. Il lato oscuro dell'IA*, il Mulino, 2021

M. Cuniberti, M. Bassini (2022), *I servizi di media audiovisivi*, in G.E. Vigevani, O. Pollicino, C. Melzi d'Eril, M. Cuniberti, M. Bassini, "Diritto dell'informazione e dei media", II ed., Giappichelli, 2022, pp. 359-392

G. De Gregorio (2022), *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, 2022

G. De Minico (2019), *Il* favor minoris*: un orizzonte lontano*, in G.B. Abbamonte, E. Apa, O. Pollicino (a cura di), "La riforma del mercato audiovisivo europeo", Giappichelli, 2019, pp. 99-124

B. De Witte (2023), *Soft Law in European Public Law*, in M. Eliantonio-E. Korkea-aho-U. Mörth (eds.), "Research Handbook on Soft Law", Edward Elgar Publishing, 2023, p. 101-115

F. Donati (2019), *La tutela dei minori nella direttiva (UE) 2018/1808*, in G.B. Abbamonte, E. Apa, O. Pollicino (a cura di), "La riforma del mercato audiovisivo europeo", Giappichelli, 2019, pp. 125-137

O. Grandinetti (2022), *Le piattaforme digitali come "poteri privati" e la censura online*, in L. Abba, A. Lazzaroni, M. Pietrangelo (a cura di), "La Internet governance e le sfide della trasformazione digitale", Editoriale scientifica, 2022, pp. 231-249

O. Grandinetti (2021), *Articolo 2*, in C. Contessa-P. Del Vecchio (a cura di), "Testo unico servizi di media audiovisivi", La Tribuna, 2021, pp. 286-304

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, pp. 35-51

R. Niro (2021), *Piattaforme digitali e libertà di espressione fra autoregolamentazione e coregolamentazione: note ricostruttive*, in "Osservatorio sulle fonti", 2021, n. 3, pp. 1369-1391

T. O'Reilly (2005), *Web 2.0: Compact Definition?*, in "Radar", 1 October 2005

M. Orofino (2014), *La libertà di espressione tra Costituzione e Carte europee dei diritti*, Giappichelli, 2014, pp. XXI-280

M. Orofino (2008), *Profili costituzionali delle comunicazioni elettroniche nell'ordinamento multilivello*, Giuffrè, 2008

O. Pollicino (2021), *Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?*, Hart, 2021

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, pp. 3-24

M. Santaniello (2022), *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, in L. Abba, A. Lazzaroni, M. Pietrangelo (a cura di), "La Internet governance e le sfide della trasformazione digitale", Editoriale scientifica, 2022, pp. 63-68

H.-W. Micklitz, O. Pollicino, A. Reichman et al. (eds.) (2021), *Constitutional Challenges in the Algorithmic Society*, Cambridge University Press, 2021

G. Scorza (2022), *In principio era Internet e lo immaginavamo diverso*, in L. Abba, A. Lazzaroni, M. Pietrangelo (a cura di), "La Internet governance e le sfide della trasformazione digitale", Editoriale scientifica, 2022, pp. 23-26

G.E. Vigevani, O. Pollicino, C. Melzi d'Eril et al. (2022), *Diritto dell'informazione e dei media*, II ed., Giappichelli, 2022

M. Villone, A. Ciancio, G. De Minico et al. (a cura di) (2012), *Nuovi mezzi di comunicazione e identità: omologazione o diversità?*, Aracne, 2012

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0140 • articolo sottoposto a peer review • pubblicato in anteprima il 4 giu. 2024

Teresa Balduzzi – Livia Siclari

Participative and Deliberative Democracy Facing Technology
A Study on Digital Democratic Innovations

The paper analyses the efficacy of digital platforms for deliberative and participatory democracy in enhancing democracy. After examining the concepts of deliberative and participatory democracy (§IA), particularly their meaning from a legal standpoint and their relation to representative and direct democracy (§IB), the study introduces the broader concept of 'digital democratic innovations' (§IC) and adopts a classification framework (§II). Then, the current legal framework of e-participation in Italy, Germany, France, and the EU is analysed (§III). This comparative analysis sets the stage for a detailed examination of five digital platforms operating at both local and national levels, which serve as case studies. Through a systematic evaluation of the key features of these platforms, the paper classifies those platforms according to the classification framework (§IVA-E). It also assesses the quality of citizen participation facilitated by each digital democratic innovation exploring two indicators: the meaningfulness of participation and the extent of digital deliberation (§IVF). In drawing conclusions, the paper also suggests potential avenues for further legal research into digitised civic participation (§V).

Digital Democracy – e-Participation – e-Deliberation – e-Democracy – Participatory platforms

Democrazia partecipativa, democrazia deliberativa e piattaforme
Contributo allo studio delle "innovazioni democratiche digitali"

Oggetto del contributo è la capacità "democratizzante" delle piattaforme digitali progettate per ospitare istituti di democrazia deliberativa e partecipativa. Tracciate le origini dei concetti di democrazia partecipativa e deliberativa nella scienza politica, si approfondisce il loro significato dal punto di vista giuridico, nonché il loro rapporto con la democrazia rappresentativa e gli istituti di c.d. democrazia diretta. Si introduce quindi il più ampio concetto di "innovazioni democratiche digitali", adottando un framework per classificarle. Il contributo prosegue quindi con un'analisi comparativa della regolazione della partecipazione digitale in Italia, Germania e Francia, e nell'ordinamento dell'Unione europea. Tale analisi prepara il terreno per l'esame di cinque piattaforme digitali operanti a livello locale e nazionale, classificate secondo il framework. Spunti ulteriori per valutare tali esperienze sono poi tratti dall'applicazione di due indicatori: la "partecipazione significativa" e la "deliberazione". Nelle conclusioni si suggeriscono infine alcune possibili direzioni per la riflessione giuridica in tema di partecipazione democratica digitale.

Democrazia digitale – Democrazia deliberativa – e-Participation – e-Democracy – Piattaforme partecipative

The Authors are PhD candidates in *Law & Social Change: the Challenges of Transnational Regulation* at the University of Roma Tre (Department of Law)

Introduction

I. Premises and definitions

It is a truth universally acknowledged that democracies all over the world are not in excellent shape. Widespread abstentionism, low levels of trust in politicians and decline in membership of political parties and trade unions are three visible effects of public disillusionment and disaffection with democratic institutions[1]. Whilst these indicators characterise our contemporary "age of distrust"[2], the need to democratise democracy through greater citizen participation has been long felt[3].

A. Origin and evolution of participatory and deliberative democracy

In the 1960s and 1970s, amidst student protests, some authors suggested introducing ways to enhance citizens' empowerment and self-government[4].

It was «the glaring disjuncture between the popular movements […] and academic demands

1. Smith 2009, p. 7. Literature on the 'crisis of democracy' is immense. Some authors point out that democracy intrinsically entails crisis and argue we are rather experiencing a 'dis-figuration' of the 'figure' of democracy (Urbinati 2015, p. 478); similarly, other scholars refuse the term 'crisis of democracy' as a crisis of the system per se, suggesting that «the cure for democracy's ills is more and better democracy» (Newton 2012, p. 14). As causes of this phenomenon were indicated additionally or alternatively: the crisis of political parties, the fragmentation of popular classes, the affirmation of the risk society, the rise of the new public management paradigm, public rhetoric on the ineffectiveness of parliamentary institutions, corruption. Citing Yves Sintomer, see Sorice 2020, p. 1 ff., also for further bibliography.
2. Such disillusionment gave birth to movements which "organise distrust" acting through counter-democratic modalities (e.g., forms of obstruction and censorship exercised against institutional powers, which ultimately result in putting politics on trial worldwide). See Rosanvallon 2006.
3. It is barely worth mentioning that there are also critics of extending political participation. It has been argued that «the effective operation of a democratic political system usually requires some measure of apathy and non-involvement on the part of some individuals and groups» and thus «self-restraint on the part of all groups» is necessary to replace «less marginality on the part of some groups» and avoid «overloading the political system» (these are words of the report by Crozier-Huntington-Watanuki 1975, p. 128). Similar elitist views were shared by Joseph Schumpeter according to whom every elector «as soon as he enters the political field […] becomes a primitive again» (Schumpeter 1976, p. 262).
4. Carol Pateman, Peter Bachrach and Crawford Brough Macpherson are among the protagonists of this theoretical movement.

for 'realistic' democratic theory»[5] which gave rise to the idea of 'participative' or 'participatory' democracy: this theory emphasizes the importance of citizen participation in decision-making processes at all levels of government beyond and next to institutes of representative democracy (i.e., elections at all territorial levels, participation through political parties) and institutes predominantly labelled as direct democracy (e.g., referendums)[6]. However, it was in the 1990s that the term 'participative/participatory democracy' and its translations and transliterations (*Bürgerbeteiligung*, *démocratie participative*, *democracia partecipativa*, *democrazia partecipativa*) spread among western political theorists all around the world, in the wake of Porto Alegre's experience of participatory budgeting[7].

In the meantime, the picture of doctrines and practices was further expanded by the rise of deliberative democracy. This theory «emerged as a corrective to the perceived focus on aggregative forms of democracy» and «provided a powerful theoretical critique [to such] tendency within democratic theory and practice to focus on the aggregation of preferences as the fundamental mechanism of legitimation»[8]. Then the Internet came along and the entire debate over new forms of democracy could not but being affected by it. But let us take a short step back.

Relationship and differences between participatory and deliberative democracy have long been studied by political theorists. The differences in geographical and social origin[9] affected the relationship between theory and practice which is expressed by these two concepts. On the one hand, participatory democracy focuses on practical experiences, with emphasis on social justice and the necessity to involve all citizens, including those who live on the fringes of society[10]. Definitions of the concept are quite broad[11], leading some to argue that it encompasses rather an «heterogenous, contradictory and shapeless set of aspirations, tendencies and political orientations which try with words and sometimes with concrete experiences to open a few breaches in the democratic citadel»[12].

On the other hand, deliberative democracy has deep roots in political theory reaching very high levels of abstraction[13]. We will not delve into either the different versions of deliberative theory nor into the debate over its alleged elitist nature and scarce feasibility. However, it is crucial to point out that according to deliberative democrats «public deliberation of free and equal citizens is the core of

5. Pateman 2012, p. 8. In other words, according to Pateman, the participatory democracy can be seen as a reaction to the democratic elitism mentioned in footnote 3 (see also Smith 2009, p. 14).
6. Further on the difference between participatory and direct democracy institutes, especially from a legal point of view, *infra* § B.
7. Porto Alegre was the first city to implement participatory budgeting in 1989. This is a democratic process, in which a community decides how to spend part of a public budget. Participatory budgeting has been recognised since 1996 by the UN as one of the best practices of urban governance and a vital instrument to attain sustainable human development (see Department of Economic and Social Affairs 2005, p. 1; for an internationally recognised definition of participatory budgeting see Sintomer-Herzberg-Röcke-Allegretti 2012, Article 9). It has spread all over the world, differentiating according to the legal and socio-economical systems. For a review of participatory budgeting experiences worldwide till 2018 see Dias 2018. See, among others, Allegretti 2010, p. 6.
8. Smith 2009, p. 14.
9. We mentioned that participatory democracy attracted global attention after its concretisation in the economically less developed Latin America. Deliberative democracy, on the contrary, has always had a strong western imprinting, being first theorised in North America (John Rawls) and then developed in Europe by the Frankfurt School on the wake of Jürgen Habermas' work. See Allegretti 2008, p. 178.
10. *Ibidem*.
11. According to the fortunate definition of Umberto Allegretti participatory democracy is «a relationship between society and institutions, which consists in direct expressions of the former [society] in processes of the latter [institutions]». Allegretti 2006, p. 156.
12. Bobbio 2006, p. 1; see also Bifulco 2009, p. 2; Politi 2021, p. 518 ff.
13. See Floridia 2017. For the relationship between Jürgen Habermas' theories and deliberative democracy see also Floridi 2020, p. 341 ff.

legitimate political decision making and self-government»[14]. They refuse the idea of democracy as a process of mere aggregation of preferences (for example on how to allocate a certain budget) and focus on deliberation in the original Anglo-Saxon meaning, i.e., a thoughtful weighing of options and opposing arguments before taking a decision[15]. The discussion must thus be informed (and informative) and balanced, allowing participants to change their preferences after they reach more considered opinions[16], and it must include (or represent) anyone who is affected by the decisions made. Examples of deliberative democracy practices include citizen assemblies, citizens' juries and deliberative polls.

From what previously outlined emerges that participatory and deliberative democracy are labels for a great variety of theories and practices which sometimes collide but more often overlap. Whereas the best practices of participatory democracy entail deliberation, deliberative democratic theories find their privileged – though not exclusive – realm of application in participatory democracy practices[17]. This is why the comprehensive term 'participatory-deliberative democracy' is preferred.

B. Participatory-deliberative democracy as a legal concept

Faced with the emergence of these theories and practices, jurists have sought to clarify the meaning of deliberative and participatory democracy within the realm of law. The challenges inherent in this effort are considerable, as underlined by a legal doctrine that we might call 'dogmatic'. First of all, challenges stem from the philosophical and political theory origins of these terms. Additionally, substantial variations among different authors and a notable degree of vagueness in the subject of analysis, especially among deliberative theorists, further complicate the task. Moreover, there appears to be a certain detachment from the 'principle of reality' associated with these concepts[18].

It has been suggested that deliberative democracy should be elevated to a 'normative ideal', alongside other models of democracy such as representative and direct democracy. This ideal would not be descriptive, but rather serve as a set of principles (maximum degree of inclusivity and deliberation with the goal of achieving a common stance) that legislators, administrators, and even judges should strive towards[19].

Other scholars have defined the legal notion of participatory-deliberative democracy essentially by distinguishing it from forms of democratic participation stemming from the 'traditional' representative system (including forms of so-called 'direct democracy') and forms of participation which are not 'democratic', i.e., do not concern the *démos* as a whole[20]. In this view, participatory-deliberative democracy instruments are ways of democratic participation which differ from: (*i*) the classical institutes of representative democracy (e.g., elections and participation through political parties); (*ii*) institutions predominantly labeled as examples of direct democracy (e.g., referendums)[21]; (*iii*) participation in administrative proceedings[22]; (*iv*) consultations of particular classes of stakeholders and not the general public, implying the possibility for public authorities to choose participants based on their specific interest in the matter (e.g., restricted

14. Bohman 2004, p. 23.
15. Bosetti-Maffettone 2004.
16. Fishkin-Luskin 2005, p. 284.
17. See Allegretti 2010, p. 16 ff.
18. Bifulco 2017, p. 3.
19. *Ibidem*.
20. Di Folco 2023, p. 300.
21. Some scholars, while underlining the importance to integrate the representative 'trunk' of democracy with 'branches' of participation, contend that institutes traditionally studied as examples of 'direct democracy', such as the referendum, are examples of participatory democracy embedded in a representative system: Luciani 2005, p. 32.
22. Which are not democratic because they are not directed to the *démos*, rather only to those who have a specific interest ('legitimate interest') in the proceeding: Di Folco 2023, p. 300.

consultations for regulatory impact assessment)[23]. Subsequently, we will adhere to this perspective. However, further clarification is necessary regarding the differences between direct democracy and participatory-deliberative democracy.

Understanding the demarcation line between these two sheds light on the specific characteristics of participatory-deliberative democracy. First of all, while institutions of so-called direct democracy permitted in contemporary systems are mostly sporadic and specific events, participatory-deliberative democracy fosters a continual relationship between citizens and institutions. Moreover, institutes of direct democracy embedded in representative systems normally involve solely individuals entitled to vote, i.e. citizens[24]. On the contrary, participatory democracy often opens up to individuals that do not possess citizenship, e.g., so-called city users[25], and sometimes to representatives of interest groups and local communities[26].

Furthermore, mechanisms of direct democracy can in many legal systems yield decisions of equivalent strength to representative institutions (consider, for instance, abrogative referendums). This is a goal that participatory democracy practices and deliberative democracy theories do not seek to enact[27], acting on a different theoretical and practical plane: in most cases, decisions remain ultimately in the hands of the promoting (administrative and/or representative) institutions, thereby attributing a 'consultative' nature to participatory-deliberative practices[28]. Nevertheless, institutions are bound to take the outcomes of the participatory process into consideration and to provide a precise rationale if they choose to contradict the decisions made within that process[29]. Additionally, there are some interesting exceptions to the 'consultative' nature of participatory-deliberative practices: for example, participatory budgeting, where citizens can decide on the allocation of a small portion of the budget, formulating proposals and voting them[30].

In conclusion, we believe that it is possible to distinguish participatory-deliberative democracy instruments from other forms of democratic participation. Essentially, these instruments serve as 'branches' to the 'representative trunk', and could help reinvigorating its roots too[31]. The concept encapsulates a variety of participatory instruments, yet it is not immune to grey areas. In particular, it can be challenging to distinguish between genuine participatory-deliberative practices and consultative practices which could degenerate in mere 'opinion polling' conducted by institutional players. Such consultative practices tend to essentially validate decisions already established by governing authorities, thus morphing into «techniques and procedures for depoliticizing decision-making processes» instead of acting as «instances of politicization»[32].

C. Digital democracy and digital democratic innovations

Meanwhile political theory has moved forward. Nowadays many scholars refuse to embrace a specific democratic theory and prefer a comprehensive approach which broadens the scope of research to all 'democratic innovations', including but not limited to participatory and deliberative experiences. Under the term 'democratic innovations' all «institutions that have been specifically

23. Di Folco 2023, p. 294.
24. Nevertheless, there are some significant exceptions; for instance, in Italy, EU citizens, who do not possess Italian citizenship, can participate in elections for the local council and in elections for the European Parliament.
25. See *infra* § IV A.
26. Vilain 2010, p. 299 ff.
27. See Villaschi 2022, p. 93.
28. See Allegretti 2010, p. 13. According to the author, such institutions are «therefore not at all deprived of their role, but this role takes on a different form compared to purely representative and bureaucratic procedures, as they must accept the autonomous interaction of the public».
29. Allegretti 2011, p. 12.
30. An example of participatory budgeting will be analysed in § IV A.
31. Balduzzi-Servetti 2017, p. 78 ff.
32. Citing N. Urbinati see Sorice 2020, p. 5.

designed to increase and deepen citizen participation in the political decision-making process» are to be understood[33]. This way, the category encompasses also instruments commonly labelled as examples of direct democracy (e.g., referendum)[34].

Furthermore, Graham Smith's definition itself has been criticised for being too restrictive, due to its emphasis on institutions and techniques, which some argue makes it «fundamentally top-down» in its approach[35]. This is why more inclusive definitions of democratic innovation encompassing bottom-up forms of participation seem now widely accepted by scholars. According to Kenneth Newton a Democratic Innovation is a «successful implementation of a new idea that is intended to change the structures or processes of democratic government and politics by improving them»[36].

Among democratic innovations most scholars agree that 'electronic democracy', also called 'e-democracy' or 'digital democracy', holds a special place. While some argued that digital democracy constitutes something qualitatively different which would revolutionise and substitute contemporary forms of democracy leading to an 'electronic democratic deliberative democracy'[37] most scholars agree that it rather identifies the use of digital tools to implement various forms of democracy[38].

Preliminary, it is worth noting that e-democracy differs from e-government which is defined by the United Nations as "the use of ICTs to more effectively and efficiently deliver government services to citizens and businesses". The concepts of e-democracy and e-government are often used interchangeably and, at times, intentionally misleading[39]. While acknowledging that in certain contexts the terms may overlap[40], it can be asserted that e-government, unlike e-democracy, puts emphasis on the efficiency of the State and regards cit-

33. Smith 2009, p. 5.

34. *Ivi*, 215 ff. For the opinion according to which the referendum is an instrument of participatory democracy in a broader sense, see footnote 21.

35. Sorice 2020, p. 2.

36. Newton 2012, p. 15.

37. See, among others, Grossman 1996. It is the myth of ICT-enabled direct democracy that completely substitutes representative democracy. The rhetoric of some political movements like the 5 Star Movement in Italy or the Spanish *indignados* propagate a sort of 'hyper-democracy' – which could degenerate in a 'click-democracy'. Partially different some initiatives of the German Pirate Party, linked to the idea of "liquid democracy". The software used by the Pirate Party, LiquidFeedback, allows for 'liquid' delegation, i.e., delegation to another person of the power to decide on a particular topic, which could be given in turn to another person and so on. See Chiusi 2014. Further on LiquidFeedback and its limits, in Gometz 2017, p. 179 ff.

38. Beacon 2021. A critical approach to ICT for democratic innovations allows to transcend the debate between digital 'optimists' and 'pessimists'. For a review of the debate over time see Sorice 2021, p. 40 ff. For a definition of e-democracy as «the use of ICT as means to carry out egalitarian procedures of self-government of the demos» see Gometz 2017, p. 20 ff.

39. Sorice 2021, p. 63. The author also contends that e-government is a way to legitimize neoliberalist tendencies among governments.

40. Gianmarco Gometz, for example, identifies an overlap between «genuinely democratic forms of e-government» and forms of «electronic participatory democracy». The author starts by defining e-government as «the use of ICT to adopt, implement, or evaluate decisions linked to the implementation of general and abstract norms adopted by the legislator». Then he suggests that e-government can be considered 'democratic' when it involves citizen participation in the adoption or, at the very least, the evaluation of decisions related to achieving the legislator's goals. However, to be genuinely democratic the contribution from the public must be effective and compelling for public institutions (or at least not easily derogable). Following this, Gometz draws on the distinction made by Umberto Scarpelli between 'government democracy' (*democrazia di governo*), i.e., involving democracy decisions concerning very general interests and where individuals act as components of the main political institution; and 'participatory democracy' (*democrazia partecipatoria*), i.e., involving decisions about 'less general purposes', distinguishing citizens based on their specific relationships with territorial entities or

izens more as clients/users rather than as subjects with political rights. The term 'digital democratic innovations' will be employed hereafter as it is the most comprehensive way to approach all examples of Democratic Innovations, in the broader sense described by Kenneth Newton, by which the digital compound plays a significant role. Digital democratic innovations are primarily enacted through digital platforms, which we denote as 'participatory platforms' or 'platforms for citizen participation'.

II. Adopting a framework to classify digital democratic innovations

To approach digital democratic innovations we adopt the framework developed by Fiorella De Cindio and Andrea Trentini (Fig. 1, from now on, simply the "Framework") in their book *Cittadinanza digitale e tecnocivismo – II volume*[41]. Moving from the perspective of informatics[42] and drawing inspiration from Sherry Arnsteins's *Ladder of citizen participation*[43], the authors identified eight layers, or 'levels' of digital citizenship, each of a different colour, forming a metaphorical rainbow. The primary goal is to investigate the impact of ICT on active citizen participation. This endeavor involves classification[44] of participatory platforms, as this categorisation serves as the initial step towards evaluation, i.e., investigating whether and to what extent these tools serve the purpose to democratise democracy.

The first group of 'technological-infrastructural' levels is deeply connected to the problem of digital divide, which is a major challenge to the implementation of digital democratic innovations. The second group of layers, covering the 'participative' levels, addresses the heart of online civic participation and Digital Citizenship.

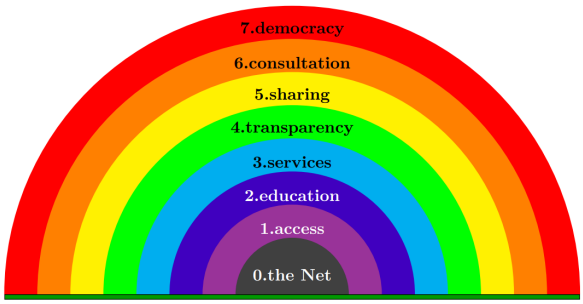


Fig. 1 — *Digital Citizenship's raibow in the digital era (De Cindio-Trentini 2024)*

- Level 0 [*the Net*]: essential infrastructure which must entail two characteristics, i.e., openness and neutrality.
- Level 1 [*access*]: access to any kind of internet connection is not enough. Today we expect fast, reliable, well-connected networks (such as fibre optic), free wi-fi and coverage over 90% of the territory.
- Level 2 [*education*]: improving citizens' digital skills is key to enable them to access the services provided by public administration.

non-territorial institutions and intermediary bodies. Finally, the author introduces the concept of 'participatory electronic democracy', which requires «active citizen involvement in collective decisions related to the specific way of achieving the goals determined at the level of government democracy». He thus identifies an overlap between forms of participatory electronic democracy and genuinely democratic forms of e-government. See Gometz 2017, p. 35 ff.

41. The book is currently being published. The framework was first presented with some minor differences in two articles (De Cindio-Sonnante-Trentini 2012, p. 1 ff.; De Cindio-Trentini 2014, p. 403). In Trentini-Biscuolo-Rossi 2020 a slightly different framework is presented. The reasons why the Authors decided to turn back to the original version of the framework are clarified in the Introduction of the second volume.
42. Defined as an empirical discipline whose object is the impact of digital technologies on society, informatics sets itself apart from computer science, which is a formal discipline akin to mathematics. Much like other empirical sciences – such as physics, biology and sociology – informatics observes phenomena and tries to establish frameworks to classify research objects.
43. Arnstein 1969, p. 216 ff. According to Arnstein's "ladder", consultation is a form of tokenism (counterfeit power).
44. Classification means creating hierarchical classes and assigning characteristics to the objects within each class. See De Cindio-Trentini 2024, p. 6.

- Level 3 [*services*]: the provision of online public services (tax payment, authorisations, access to online forms, online appointment booking, etc.)[45].
- Level 4 [*transparency*][46]: sharing of information by institutions about their policy making processes, which enables citizens to hold them accountable for their decisions and actions. It is a one-way relationship, where citizens are mere recipients. Thus, it does not constitute actual participation, though being essential to any of the more complex forms of participation[47].
- Level 5 [*sharing*]: autonomous creation of citizens' networks to share information, ideas, and practices. Examples range from mere information gathering (e.g., of public events) and organisation for social action (website for supporters of a particular protest), to spontaneous social reporting[48], e-petitioning (e.g., change.org).
- Level 6 [*consultation*]: all forms of institutional 'listening' to the citizens questions, expectations, needs and opinions (in a word, their feedback), e.g., unsolicited and solicited feedbacks (e.g., spontaneous complaint e-mail to public administration, institutionalised social reporting and proper public consultations, where institutions define issues for consultation, set questions, provide information, and invite citizens to offer their views and opinions[49]). According to the authors the theoretical background of this type of initiatives can be traced in 'continuous democracy'[50]. However, among these initiatives could also be found examples of participatory-deliberative democracy practices, as defined in § I A and B.
- Level 7 [*democracy*]: it includes both ICT-enabled institutions of representative democracy (e.g., e-voting), (hybrid) participatory budgeting experiences and a number of platforms for idea gathering and online deliberation.

The Framework suggests that the levels are interconnected and rely on each other for their effectiveness. In other words, each level exports services from the level below, and provides services to the level above. For instance, e-democracy could not exist without public online services, which in turn would be meaningless without a substantial level of digital literacy (and without an internet connection, for that matter). Finally, the metaphor of the rainbow suggests that many 'grey areas' are possible, where two colours merge into each other; still each colour must be vivid, and each layer must be enough thick to guarantee effective digital citizenship and participation.

As mentioned, classifying digital democratic innovation through the Framework helps us better understand the nature and level of citizen involvement in online participation experiences and distinguish between more and less 'advanced' forms of participation. However, the political and legal

45. This is the core part of e-government as defined above.
46. Level 4 [*transparency*], Level 6 [*consultation*] and Level 7 [*democracy*] follow OECD 2001.
47. The importance of transparency in public administration (e.g., open data) has been emphasised in the rhetoric surrounding e-government. Sorice 2021, p. 88. However, true participatory communication involves more than just informing, requiring the ability to activate effective forms of participation. Therefore, although some argue that e-government includes also the practice of 'listening' to the needs of the citizens, truth is that citizens are in this case seen as customers/users of public services (e.g. when citizens' 'opinions' are collected through satisfaction surveys). Thus, these practices have little to do with the 'feedbacks' mentioned in Level 6 [*consultation*], although sometimes discerning between opinion polling and satisfactory surveys may not be easy. In brief, the concept of e-government as defined above could embrace some but not all practices of Level 4 [*transparency*] and hardly includes any practices of Level 6 [*consultation*].
48. Institutionalised forms of social reporting are rather to include in Level 6.
49. OECD 2001.
50. Theorised by Stefano Rodotà in Rodotà 1997. The idea behind continuous democracy is that the gap between elections is becoming increasingly long, given contemporary acceleration in social, environmental and digital change. By actively listening to citizens on specific topics, institutions can gain a deeper understanding of their concerns and perspectives, enabling them to potentially address their needs and opinions more effectively – only if they choose to do so. For a partly different concept of 'continuous democracy' (in French, *démocratie continue*) see Rousseau 2020.

consequences descending from the utilisation of these platforms are contingent on the specific context in which they are applied[51]. Hence, after the initial classification through the Framework, which acts as a foundational step in the evaluation process, it becomes crucial to analyse the particular democratic context in which various participatory platforms are implemented. In the paragraph 'Case Studies', we examine some practical examples of digital democratic innovations, encompassing both procedures of 'democracy' (Level 7), 'consultation' (Level 6) and bottom-up experiences, thus embracing some forms of 'sharing' (Level 5). The analysis will highlight both the main features of the platforms, the legal consequences of participation, their actual use. The purpose is to discover what kind of citizen participation effectively hides behind a very similar rhetoric that makes digital democracy processes look like a homogeneous category. Before delving into the case studies is thus necessary to outline the legal framework for participatory-deliberative democracy and digital democracy in the relevant legal systems.

III. Participation in legal systems: a comparative analysis

Within the traditional framework of modern liberal democracy, the citizen is presented with few, if any, opportunities to directly influence the process of producing collectively binding decisions. And yet participatory processes can be found in societies as diverse as Indonesian and Indian villages, Swiss *Talshaften* or the classical Athenian city, where a direct model of citizenship was based upon communities in which face-to-face relationships were considered paramount. The crisis of democracy discussed above is clearly a crisis of representative democracies. According to Constant[52], one of the main differences between ancient and modern democracies is the level of direct participation: representative democracies are a direct consequence of the extention and complexity of modern States. The contemporary notion of democracy often overlaps with representative-elective democracy, since the essence of democratic systems is often deemed to be the presence of free and regular elections[53].

Nevertheless, in the last decades the need to promote new and more inclusive experiences of policy-making has emerged. In fact, it would be reductive to consider democracy just a political system in which periodically the citizens elect their representatives[54]. The principle of citizen sovereignty extends beyond the mere act of selecting political representatives. In Western legal frameworks, it is realised and developed through civic consultation practices and participatory processes. We have already stressed that contributions made by individuals or groups via those instruments are usually

51. It is worth noting that there is not a perfect alignment between the underlying democratic theory and the technological tools that serve it. The informatics perspective sheds light on the potential forms of engagement and participation the platforms *could* enable when adopted by public institutions, political parties or citizen groups. However, the consequences descending from the utilisation of these platforms derive from the specific context in which they are used. The same tool can be employed in ways that correspond ideally with different democratic theories. This imperfect overlap is particularly evident at Level 7. On the one hand, online deliberation platforms can serve as tools for public deliberation within participatory and deliberative initiatives. On the other hand, they could be used for participation through political parties thus falling within the domain of representative democracy (although the political parties itselves often advocated for a radical replacement of representative democraticy with forms of 'direct democracy' or 'liquid democracy', cfr. Chiusi 2014, p. 56 and footnote 37).
52. Constant 1992, p. 12: «Thus among the ancients the individual, sovereign almost habitually in public affairs, is a slave in all his private dealings. As a citizen he decides […] by the discretionary will of the whole of which he is a part. Among moderns, on the contrary, the individual, independent in his private life, even in the freest states is only sovereign in appearance. His sovereignty is limited, almost always suspended; and if, at fixed but rare times in which he is still surrounded by precautions and obstacles, he exercises this sovereignty, he does so only to abdicate it».
53. Trettel 2020, p. 17 ff.
54. Picchi 2012.

non-binding and serve mainly consultative purposes, given that the final decision remains a prerogative of executive or administrative institutions. Participative instruments are present at all governance levels (supra-national, national, regional and local) but, usually, the most successful can be found at regional-local level. This is, probably, due to the close proximity between civic interests and authorities in charge of the decisions[55].

It is interesting to notice how the notion of democracy has been nourished by the notion of participation since ancient Greece, evolving into contemporary democracies through a further fundamental, strengthening insertion: constitutionalism[56]. The very birth of constitutionalism, as a phenomenon that led the transition from the absolute State to the form of a liberal State can be reconstructed starting from the role of participation, as the salient facts in determining this historical evolution[57] are directly related to the progressive expansion of the legal recognition of political rights of participation of subjects, in opposition to the narrowing of the sphere of influence and power of the Crown[58]. Participation is fundamentally linked to the spirit and effectiveness of democratic Constitutions[59]: the exercise of popular sovereignty and the control of power, which call for additional instruments than those of political representation; the full development of the person and substantial equality; the increasingly pressing demand for quality and effectiveness of public policies, with regard to which the complexity of social demand calls for closer dialogue between the decision-makers and the beneficiaries of the rules. The importance of citizen participation was sanctioned, at international level, in the Aarhus Convention on access to information, public participation in decision-making and access to justice in environmental matters of 1998. Adopted by the United Nations Economic Commission for Europe (UNECE), and titled after its own pillars, it is considered not only an environmental agreement, but also a shared agreement about governments accountability, transparency and responsiveness to their citizens. In 2003, the Aarhus Convention was transposed into European Law by Directive 2003/35/EC on public participation and access to justice. A more in-depth analysis of EU framework on participation will be delivered at paragraph III D, however it is important to mention how the European legal system recognises instruments of participatory democracy that, completing the representative dynamics, are aimed at promoting the direct involvement of European citizens by increasing the legitimacy of decision-making processes in the Union and bridging the so-called EU democratic gap[60].

In Latin America, participation is not limited to the demonstration of an oppositional interest, nor limited to the vote on the adoption of a final measure. But, on the contrary, it involves any interested party to make their own deductions in the "rulemaking" proceedings in terms of collaboration with the public service. Although, in principle, general and administrative legislative acts represent the area in which the public is most involved in legislative production, the Latin American context is rather articulated on the subject. Thus in some systems, such as Venezuela and Colombia, public participation assumes the dimension of subjective law, exercisable, albeit with different intensity, in every type of rulemaking procedure. A dimension that finds, instead, a strong contraction in those experiences where there is a non inclusive approach on the subject. This is the case of Peru, which reserves the right to intervene in the definition of first-degree norms only to indigenous

55. For further analysis on this point see: Pepe 2020. Particularly interesting the author's statement about how representative democracies aggregate citizens 'by communities of neighbourhood' while participatory democracy sorts them in 'communities of interest', p. 10.
56. D'Atena 1998; Morelli 2015.
57. In England after the 'Glorious Revolution' of 1688-1689, France in the Restoration Age, Belgium with the Revolution of 1830, Italy with the Statute of 1848, Germany in the Bismarckian Age, Russia after the Revolution of 1905.
58. Referring to modern constitutionalism see Pettinari 2019.
59. Valastro 2010.
60. Martines 2023, p. 308.

peoples, while in Ecuador and Bolivia, again in relation to aboriginal communities, this restriction also concerns secondary sources and general normative acts. Participation in Chile and Argentina is rather subdued, not being formally guaranteed on the general level, but finding express discipline and stronger guarantees only in environmental matters[61]. Unlike in Brazil, that was the homeland of the first participatory budgeting experience in Porto Alegre[62], the intervention of the public assumes an atypical value and leans to deliberative democracy.

As already observed in § I, the notions of participatory and deliberative democracy have been heavily discussed by political theorists.

If it is true that participatory democracy has structural limitations that keep – and will always keep – it from replacing representative democracy[63], it is also true that citizen participation can ultimately play a useful role in democratising representation, integrating in a pluralistic and inclusive way tools, procedures and institutions rooted in representative democracy[64]. However it is worth underlining that the evolution of the Marxist-leninist ideology brought to the institutionalisation of participation both in China[65] and, especially, in Cuba. During the drafting of the Cuban constitution of 2019 the population has been involved well beyond the final referendum, through participatory consultations *Consultas Populares*[66] that involved both Cuban residents and those living abroad. Cuban citizens had the opportunity to present their personal views on the constitutional project at meetings held in the workplace, schools, hospitals and neighbourhoods[67]. On the other hand, in EU it is uncommon for Constitutions to explicitly address the concept of participation, only two constitutional charters do, i.e., the Italian and the Portuguese. In particular, article 2 of the latter, affirms that: «The Portuguese Republic is a democratic constitutional State […] that aims to achieve the realisation of economic democracy, social and cultural and the strengthening of participatory democracy». A rather non-specific and broad assertion that is nevertheless useful to underline the effort in the search for democratisation after the end of the Caetano dictatorship.

In the following paragraphs we shall outline if, where and how participation is addressed in the legal systems of the Countries of the platforms investigated in § IV.

A. Italy

Citizen participation is deeply rooted in the Italian Constitution[68]. The Constituent Assembly implied it at Article 3, when, after affirming the general principle of formal equality in the first paragraph[69] goes on to set out in the second paragraph the principle of substantial equality: «It shall be the duty of the Republic to remove those obstacles of

61. See Zinzi 2021, p. 1197.
62. See footnote 7.
63. Cardone 2021, p. 13.
64. Siclari 2009, p. 3; Tushet 2016, p. 167 ff.
65. Since the revolution the concept of people sorveignity in China was compenetrated by the idea of people participation in all public matters. See: Horsley 2009.
66. Present in both Cuban Constitutions, this mechanism serves to exercise the constitutional right to vote on issues of national importance so that their will, binding under the law, may influence the debate and decisions of the representative organs of the State.
67. At the request of the National Assembly, the project was submitted – from 13 August to 15 November 2018 – to popular consultation. There were 1,706,872 interventions and 783,174 proposals were made, 666,995 requests for modification, of which 32,149 requests for addition of new dispositions, 45,548 requests for elimination, 38,482 of doubts. There were also 2,125 proposals from Cuban citizens living abroad. In four months, 133,681 meetings were held, involving 8,945,521 (77.89% of the Cuban population) in all 15 provinces of the Country. For a deeper analysis of the Cuban constitutional drafting see: Sciannella 2020, p. 557 ff.
68. Balduzzi-Servetti 2017, p. 8.
69. «All citizens shall have equal social dignity and shall be equal before the law, without distinction of gender, race, language, religion, political opinion, personal and social conditions».

an economic or social nature which constrain the freedom and equality of citizens, thereby impeding the full development of the human person and the effective participation of all workers in the political, economic and social organisation of the country».This was meant to mark a distinction between the former Italian monarchy, as well as the fascist regime, and the post-war egalitarian republic. At the same time, the constituents chose to link the concept of participation to the larger principle of substantial equality in order to avoid an excessive indefiniteness. The breadth of the concept of participation concerned the constituents, and in fact only in more recent times scholars further refined the concept of participatory democracy, delineating its boundaries[70] and excluding participation to the administrative proceeding[71], institutions mostly referred to as direct democracy such as abrogative referendum[72] and legal instruments for the consultations of stakeholders[73].

After the reform of Title V of the Italian Constitution, citizen participation is expressly addressed at paragraph 4 of Article 118 that now recites: «The State, regions, metropolitan cities, provinces and municipalities shall promote the autonomous initiatives of citizens, both as individuals and as members of associations, relating to activities of general interest, on the basis of the principle of subsidiarity»[74]. This addition is rich in implications, especially in terms of constitutional foundation of the direct management of public affairs (carrying out activities of general interest) by subjects traditionally not included in it[75]. The principle is not detached from other content of the constitutional text, and its explicit inclusion in the Constitution represents the point of arrival of a path that – started with national and communitarian regulations – has marked a phase of juridical positivisation that collects a wide variety of historical-cultural and institutional heritage.

A further development has occurred with the *Codice dell'Amministrazione Digitale* (CAD, Code of Digital Administration)[76], where a 'digital administration' – as both a legal and organisational concept – evolves from a mere structure of employees, procedures etc. into a complex, connected, ICTs equipped management system, allowing documentation to be processed and processes to be managed computer-based, ultimately benefitting citizens and businesses with both faster and new services. In addition to the most practical aspects and the general spirit of technical modernisation of the Public Administration (PA) CAD Article 9 translated the principle of participation in the digital age stating that: «The State encourages all forms of use of new technologies to promote greater participation of citizens, including those living abroad, in the democratic process and to facilitate the exercise of individual and collective political and civil rights». It is clear, however, that for the implementation of these processes, there has to be formal recognition or institutionalisation through

70. Trenta 2022, p. 95 ff.

71. According to Law no. 271/1990 this kind of participation rooted in a subjective position, legitimate interest, which is articulated in specific powers of intervention during the procedure.

72. Which is expression of the right to vote based on article 48 of the Italian Constitution and lacks a moment of exchange and confrontation on the arguments.

73. Such as the Houses' of Parliament consultation procedures in the legislative process or restricted consultations in the regulatory impact analysis. See: Bifulco 2009, p. 66 ff.

74. Hereby intended as *horizontal subsidiarity* based on the assumption that the taking care of collective needs and general interest activities is provided directly by private citizens (both as individuals and as associates) and that public authorities act as 'subsidiaries,' planning, coordinating and, where appropriate, managing these initiatives.

75. According to some scholars, subsidiarity does not entail participation to a process that culminates with a decision of the representative or administrative authorities, but only in the implementation activities of general interest by individual and associated citizens.

76. Established by Legislative Decree of 7 March 2005, No. 82, was subsequently amended and supplemented first with Legislative Decree No. 179 of 22 August 2016 and then with Legislative Decree No. 217 of 13 December 2017 to promote and make effective digital citizenship rights.

consolidated procedures and *ad hoc* rules yet to be declined. Surely, a desirable institutionalisation must pass through the creation of new instruments of participation, both in the administrations themselves and at the political decision-making level[77].

B. Germany

In Germany, the Fundamental Law sets several principles that serve as legal foundation and boundaries to participation, but it does not contain an express reference to participatory democracy. On its own the democratic principle would not suffice to be a legal basis to public participation; Article 20 I establishes that «All state power emanates from the people. It is exercised by the people through elections and votes and through special bodies vested with legislative, executive and judicial powers», but otherwise there are very no references to participatory democracy instruments, due to the traumatic experiences of the Nazi regime[78]. However, the Federal Constitutional Court has endeavoured to broaden some of the Fundamental Law principles in order to keep it up with the pace and the spirit of the time[79].

The multiplication of participatory procedures to the administrative decision process, involving an increasing consideration of the subjective rights of the citizens, is a sign of the increased importance of the relationship between the administration and its users, since these means «allow to take part in the powers of the State itself, as well as asserting and exercising one's rights»[80]. Right to participation as stated in Article 20 not so much resulted in guarantees of participation in the legislative process, but rather in the administrative process and thus in the relationship between the public and the administration, from which the relevance of the sub-state level – and in particular the municipal level – derives, given the nature of administrative/enforcement federalism of the German system. In this framework, then, forms of participation of experts or subjects directly affected by the decision are juxtaposed with forms of participation of an inclusive nature that provide for a genuine consultation of the community to which the decision refers. Also, the federalist nature of Germany facilitated the affirmation of participatory democracy, allowing to increase the opportunities to foster participation at a regional and local level.

The German Federal Emission Control Act was passed in 1974 and was one of the first laws containing a formal procedure that enabled the public to raise objections during the planning phase. In 1976, a similar clause on early public involvement was introduced in the German Federal Building Code. Subsequently, several pieces of German legislation have further expanded of this issue. The German Environmental Appeals Act of 2006 enables approved environmental NGOs to appeal in court administrative decisions. Finally, with the 2013 Germany Administrative Procedure Act[81] a new Section 25 (3) on early public participation was passed. It provides for a set of mandatory early public consultations in several matters. Some other examples of typical participatory instruments in Germany are the *Bürgerversammlung*, *Bürger-befragung*, *Anhörung*, *Bürgerforum*, *Planungszelle*, *Bürgergutachten*, *Zukunftswerkstätte*[82]. Each of these procedures may be formal in nature – i.e., expressly regulated in legislative acts – or informal – having been developed and established through practice.

C. France

Conversely, for most of other EU Countries, the process has gone in reverse order starting from normative sources of primary rank in absence of explicit constitutional formalisation. For example, France has been one of the most attentive countries in the past decades when it comes to preven-

77. Carloni 2019.

78. Understandably, in a Country where citizens organisations had gained such power as to subvert the existing institutions. Vilain 2010, p. 305.

79. BVerfGe 21, 378 (388).

80. For example, the constitutional court added material elements such as the "idea of justice," the realisation of which requires in particular the adaptation of the procedural law. See: Guerard 2007.

81. Verwaltungsverfahrensgesetz, VwVfG.

82. Citizens' assembly, citizens' survey, hearing, citizens' forum, planning cell/citizens' report, future workshop.

tive consultation with stakeholders through two instruments: *enquête public* and *débat public* (the latter implemented through consultations and concertations)[83]. Both of them are meant to enrich public policymakers awareness of the social interests involved in their decisions. Traditionally, French law limited public input to the public inquest[84] where the prefect of each department is in charge of organizing the procedures. Since its reform in 1983, the inquest includes a form of public consultation open to all, but does not include a public debate. The task is to inform the population of regional projects, both public and private, and to assist the prefect himself in making the final decision on the approval of the project. It is compulsory for projects that include the taking of private property and in 2011 was expanded to include projects that have an impact on the environment. The process is, essentially, a way for the national government to exert some control over spending priorities and economic development at local and regional levels[85].

Only in the 1960s participation became a major aspect of public administration reform, as a mean to regenerate bureaucracy and also to foster social and political links. The principle of participation was formally introduced for the first time in 1995 with the *Loi Barnier* on the reinforcement of environmental protection. It assesses that a public debate on the objectives and main characteristics of the projects could be organised, during the development phase of major public development operations of national interest, by the State, local and regional authorities, public institutions and mixed economy companies with a strong socio-economic stake or with a significant impact on the environment.

In addition to that, a great innovation was the institution in 1997 of the *Commission nationale du débat public* (CNDP - National commission on public debate), in charge of overseeing organisation modalities and the regular execution of the public debates that would be launched[86]. The CNDP seeks to apply principles of inclusion, argument and openness. The aim is a process that allows a broad range of public concerns to be vetted and discussed before the government settles on a particular plan.

The fundamental value of the principle of participation was then recognised in Article 7 *Charte de l'environnement*[87], that gained constitutional value following a series of decisions of the Constitutional Council[88]. Finally, the novation of the legal framework, under the effect of the constitutionalisation of environmental rights – with its inclusion in the preamble to the Constitution – and duties in 2005 and the creation of the procedure of the priority question of constitutionality in 2008, was a powerful factor in promoting the principle of participation[89]. Also, the Conseil d'Etat 2011 Report on participation advocates a process where the government frames the issues in general terms, followed by an open ended concertation, an impact assessment inside the government and a more formal consultation at the end. This is the scheme adopted when designing the French platform for public debate that will be analysed in § IV.

83. Consultations refers to consultations with stakeholders bodies, with close membership and strong impact of their views on public policy, representing various interests. Concertation refers to an open-ended consultation in which there is a real discussion with concerned citizens and organised groups.
84. The first law on public inquests dates from 8 March 1910 and simply allowed landowners to comment on proposed projects that involved the taking of their land.
85. Rose-Ackerman-Perroud 2013, p. 307.
86. The CNDP is composed by 25 members drawn from a range of interest groups and political bodies, e.g., prefects, State counsels, politicians, environmental and consumers groups. See Mansillon 2006.
87. «Everyone shall have the right, under the conditions and within the limits laid down by law, to access environmental information held by public authorities and to participate in the formulation of public decisions having an impact on the environment».
88. See Cons. const. n° 2008-564 DC of 19 June 2008, *Loi sur les OGM*; Conseil d'État, 3 October 2008, *Cne d'Annecy*; repealing legislative provisions which ignored the prescription of the Charte and obliging the legislator to comply its conditions and limits. See also: Chevallier 2011; Chevallier 2006.
89. Van Lang 2014.

D. European Union

Before moving on to the analysis of the platforms which serve as case studies, let us briefly outline the role of participation in the European Union.

To start, the principle of participation did not start affecting European Union Law until the late 1990s. After being a non-issue for several decades, the role citizens should play within the Union became central to EU political discourse back at the end of last century at the first European Social Policy Forum, when the Commission Directorate for Employment, Social Affairs & Inclusion launched a 'civil dialogue' with the declared dual aim of linking the views of EU citizens to EU institutions, and to explain political discourse to the public. In the same year, the 1997 Treaty of Amsterdam had for the first time established an obligation of European Institutions to adhere to the principles of democracy. It is in the 2000 Commission White Paper on European Governance that citizen participation was recognised as one of the pillars of good governance well beyond the social policies. Citizen participation throughout the entire policy cycle was highlighted as key to ensure the quality, relevance, and effectiveness of EU policymaking. Finally, with the Treaty on the European Union (TEU) Article 11[90], participation in decision making – beyond political representation – shall be considered one of the foundations of democracy in the EU[91].

In this paper, we have opted not to delve into the impact on democratic participation of social networks and other platforms that were not intended specifically for that purpose. Rather, our analysis focuses on e-participation platforms specifically created for such activities.

However, in the conclusion of this paragraph we are going to acknowledge the impact of social networks on democracy, the awareness of which has brought a consequential evolution on EU regulations. Starting with the adoption of the GDPR regulation, EU institutions adopted a human-centered approach to the 'shaping of EU digital future', very different from those adopted by China or the US, where the main focus has been the market implications, rather than the protection of individual rights and freedoms[92]. Whilst other EU regulations (GDPR, Data Act, Digital Markets Act, AI act)[93] address various aspects of the concerns raised by technological developments in the life of citizens and in the European digital market, the full-scale usage of internet services compelled the EU legislator to address this reality in a comprehensive manner from the main point of view of consumers' protection with the Digital Service Act (DSA)[94]. As citizens' participation is widely expected to take place in accordance with the newest trends, regulation over digital platforms and online service providers (*in primis* social networks) will inevitably, and deeply, impact the integrity and the unfolding

90. «The institutions shall, by appropriate means, give citizens and representative associations the opportunity to make known and publicly exchange their views in all areas of Union action. 2. The institutions shall maintain an open, transparent and regular dialogue with representative associations and civil society. 3. The European Commission shall carry out broad consultations with parties concerned in order to ensure that the Union's actions are coherent and transparent. 4. Not less than one million citizens who are nationals of a significant number of Member States may take the initiative of inviting the European Commission to submit any appropriate proposal on matters where citizens consider that a legal act of the Union is required for the purpose of implementing the Treaties».

91. Mendes 2011.

92. Raffiotta 2023, p. 248, argues that the enthusiasm of the EU lawmakers has slipped into a challenging over-regulation.

93. The strategy is set out to do this through three fundamental pillars 'technology at the service of people'; a 'fair and competitive digital economy'; and an 'open, democratic and sustainable society' all aimed at making the Union 'a global standard for the digital economy' making them also support 'developing economies in digitization' setting digital standards and promoting them internationally. See the official website of the European Commission.

94. 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).

of the public discourse. The very fact that the preamble of the DSA[95] explicitely lists the "democratic process" as one of the target of those risks that providers are directed to assess and mitigate, indicates that in the eyes of decision-makers the boundaries between the "consumer" and the "citizen" are rapidly fading, towards and endpoint at which differences among the two not necessarily could be told apart[96], at least from a practical standpoint. There are at least two factors why this is happening:

– Use of the internet
  Presently, a substantial portion of human activities is facilitated or made feasible through internet-based platforms, engendering a transformation in user perceptions. Users now perceive these platforms not only as conduits for everyday transactions but also as integral avenues for exercising civic rights and accessing essential information, job prospects, and social engagements. Consequently, the expanding influence of these corporate entities has transcended conventional consumer-provider dynamics, resulting in a nuanced blending of citizenship and consumerism, thereby obscuring traditional distinctions between these roles.
– "Politicisation" of the main corporations
  Over the last decade, virtually all main digital actors, spanning from Facebook, to X (formerly know as "Twitter") and Amazon, have frequently found themselves in confrontations with political authorities on a multitude of fronts, including privacy protection, collaboration with law enforcement agencies, surveillance of harmful content, management of hate speech, and antitrust issues. Digital firms, in response to concerns voiced by governments and citizens alike, have adopted positions on various regulatory matters pertinent to their primary operations. Consequently, the regulation of these corporations effectively entails the regulation of individuals' behavior.

The presence of notions such as 'illegal content'[97] and 'disinformation' in the DSA clearly acknowledges this new 'cross-sectional' approach refusing an excessive and obsolete partition between the 'civic' and 'economic' status of the users, thereby establishing a principle of transparency and accountability within digital platforms that facilitate public participation.

In light of the legal frameworks just outlined it can be argued that, even if political and legal theories have attempted numerous definitions, the actual realisation of participation remains free within the compliance with national regulations. Both the legal and political context, according to the country of reference, change the way participation is considered and also its grounds, and thus changes also the role of the several participatory institutes. Institutes which may, depending on the context, be classified as institutions of participatory or deliberative democracy. This stems not only from political and sociological differences between Countries, but also from the fact that participatory institutions, originating from practical experiences, have only found partial institutionalisation and are regulated in detail only in some instances, often found in local statutes.

IV. Case studies

In this section of the paper we proceed with a comprehensive analysis of five different e-participation

95. Recital 81: «A third category of risks concerns the actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, as well as public security». Furthermore, Recital 104: «(…) Another area for consideration is the possible negative impacts of systemic risks on society and democracy, such as disinformation or manipulative and abusive activities».

96. In this sense, Recital 95: «Very large online platforms or very large online search engines should ensure public access to repositories of advertisements presented on their online interfaces to facilitate supervision and research into emerging risks brought about by the distribution of advertising online, for example in relation to illegal advertisements or manipulative techniques and disinformation with a real and foreseeable negative impact on public health, public security, civil discourse, political participation and equality».

97. Broadly defined as: «… any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law»: Article 3, letter *h*), DSA.

platforms, encompassing both local and national levels. Our examination delves into the features, effective utilisation and political and legal consequences of each initiative, aiming to shed light on their effectiveness in fostering democratic participation.

A. #ROMADECIDE

In 2019 participatory budgeting[98] was implemented by the city of Rome, i.e., *Roma Capitale*[99]. The project was known by the hashtag #ROMADECIDE ('Rome chooses') and built on a previous experimental participatory budgeting project concerning one of Rome's sub-local administrative units (from now on, 'municipalities')[100]. The Statute of Roma Capitale (Article 8-bis) formally introduced it as a top-down participatory process, as per the Resolution of the Capitoline Assembly No. 5 dated 30 January 2018. The aim was to ensure «the widest popular participation and the highest level of direct democracy and transparency» also with the help of technological means[101], in line with Roma Capitale Digital Agenda 2017-2020. A special Regulation of the *Bilancio Partecipativo* was then approved on 4 April 2019[102], which defines it as both an «instrument of public participation and consultation aimed at increasing citizens' trust in institutions» and a way to improve «efficiency and effectiveness of the strategic-operational and economic-financial planning» of public administration (Article 1, paragraph 2).

The Regulation envisages the creation of a special platform for taking part to #ROMADECIDE (Article 2). The participatory platform was simply a dedicated section on the Roma Capitale institutional website[103]. According to Article 6 of the Statute of Roma Capitale, not only citizens of Rome[104] can take part to the participatory budgeting, but all city users[105]. This category encompasses non-resident citizens[106] and foreigners[107], provided they work or study in Rome[108]. Access to the service is provided through the Digital Identity System (SPID) (*Sistema Pubblico di Identità Digitale*, Public Digital Identity Management Service)[109] or using an Electronic Identity Card (CIE), thus ensuring

98. See footnote 7.

99. Roma Capitale is a special administrative body which administrates the Comune (commune) of Rome, capital of Italy. It was established in 2010 in accordance with Article 114, paragraph 3, of the Italian Constitution.

100. We refer to the participatory process of the 8th Municipality established by the Resolution of the Giunta Capitolina (governing body of Roma Capitale) No. 87 of May 2018 and aimed at deciding how to allocate 17 million euros in projects concerning environment, landscape, sustainable mobility and accessibility, urban regeneration and infrastructure.

101. See the original document.

102. See the original document.

103. Little is known of the provider of the platform. Apparently none of the big digital platforms.

104. Registered in the electoral rolls of Roma Capitale.

105. See the Document of Participation, paragraph 2.1.

106. Enjoying active electoral rights.

107. Legitimately residing in the territory.

108. According to the Document of Participation, p. 10, to verify if users were truly entitled to participate, an automatic comparison with the electoral rolls (for residents) and the request of a self-declaration, with provision for spot check (for city users), were carried out. In addition to citizens and city users, Municipalities themselves are invited to participate in the *Bilancio Partecipativo.* The act adopted by the governing body of Roma Capitale to regulate scope and procedures of the *Bilancio Partecipativo* of 2019 reserves to proposals promoted by Municipalities 20% of the budget allocated to their territory (Deliberation of Giunta Capitolina No. 103 of 31 May 2019). This provision was meant to allow co-planning and cooperation at sub-local level and to give voice to parts of population who are not digitally trained.

109. The Italian public identity system provides a unique verified account to citizens, allowing access to any on-line service of the PA as established by Article 64 CAD. A SPID account can be issued by so called Identity Providers, i.e., private and public entities accredited by the Italian Digital Innovation Agency.

identification of the participants, and preventing multiple voting[110].

From 10 June to 21 July 2019 participants could submit their proposals on how to allocate the available resources (20 million euros). Their proposals had to be in line with the project's scope, i.e., urban enhancement, and include a title, a brief and a detailed description of the action proposed, type, scope, cost, beneficiaries, and geolocation of the intervention. To protect the creators' privacy, proposals were published using aliases assigned to each creator. Each participant could publish up to 5 own proposals and support those of the other users simply by liking them, as if it were a post on a social network.

Proposals which gained at least 5% likes in each municipality were admitted to the next phase[111]. This consisted in a technical-administrative-financial evaluation by a board of administrators. The board considered valid 938 out of 1.481 proposals (plus 40 proposals presented by municipalities) and admitted 233 proposals to the evaluation (based on the rankings). By the end of its task, the board had selected 73 proposals submitted by citizens and 38 proposals submitted by municipalities to advance to the final voting stage.

The final consultation took place on the same participatory platform, accessible by previous identification. From 12 to 21 October citizens could express up to three preferences. Around 17,000 citizens took part to the final stage, 0.77% of the population of age of Rome (around 2.2 million people)[112]. At the end, 65 proposals were chosen and a Deliberation of the *Giunta Capitolina*[113] acknowledged the results and declared the end of the project. Subsequent reporting on the state of the art of the implementation of the winning proposals is provided on the Roma Capitale portal.

As a participatory budgeting experience, it falls under Level 7, Democracy, according to the Framework presented in § 1.

B. PartecipaMi

PartecipaMi is a participatory platform which aims at providing citizens of Milan[114] and their representatives «with spaces and tools for participating in the life and management of the city»[115]. It is first worth highlighting the bottom-up origin and nature of the project, in contrast with the majority of contemporary e-participatory experiences both in Italy and abroad[116]. The platform was indeed

110. On the other side, complex authentication procedures could discourage participation. It must be therefore carefully pondered whether to foresee "strong" (SPID) or "weak" (e-mail, password, normally assisted by double-check in electoral registers for residents or self declaration and possible random checks for city users). Cfr. De Cindio-Trentini 2024, p. 24.

111. With the issuance of Deliberation No. 150 of 31 July 2019 additional proposals were admitted to address vote splitting in municipalities with high levels of participation.

112. Advertisement was of course essential to foster participation: posters were displayed in particular in train and underground stations, radio ads were broadcasted, posts were made on institutional Facebook and X profiles and on the website, and in-person assistance was provided at public relation offices.

113. No. 284 of 10 December 2019.

114. It is worth noting that #ROMADECIDE addressed people living in the Comune of Rome, which spans a much wider geographical area than the Comune of Milan. To be precise, #ROMADECIDE covers an area of 1.285.31 km^2, which is significantly larger than Milan's 181.8 km^2, and has a population of approximately 2.8 million people, which is double the population of Milan's 1.4 million inhabitants. However, the platform PartecipaMi appears to serve both the Comune of Milan and its sub-local administrative bodies (municipalities), as well as the broader metropolitan area of Milan, which encompasses a population of approximately 3.25 million people, spanning across 133 communes and covering an area of 1,575.65 km^2.

115. See PartecipaMi website.

116. From June 2021 the Comune of Milan has also its own institutional participatory platform, Milano Partecipa, which is based on the open source software Decidim (see, *infra*, § III D). The launch of the platform went together with the modification of the Regulation for the implementation of popular participation rights by resolution of the Municipal Council No. 73 of 23 July 2021 (available in Italian). Alongside pre-existing

created by Fondazione RCM[117], a non-profit organisation established in 1998 to promote citizen participation using IT tools. It built on a platform which was tested experimentally during the run-up to local elections in 2006. As part of a project funded by the Ministry for Innovation and Technology, and with the support from the Lombardy region, the Fondazione RCM, in collaboration with the Civic Informatics Laboratory at the University of Milan, developed openDCN, a new open-source software platform. It was tested in a range of projects[118] linked to partecipaMi and further refined in preparation for the local elections in Milan in 2011. After the elections partecipaMi could be moved to the openDCN software.

Since 2014, the platform has been solely supported by citizens and has not received any public funding, which has helped to maintain its formal independence. Equal participation and dialogue between citizens and decision-makers (members of the City council and sub-local councils) is a key characteristic of the whole project. Registration with name and surname is required since participants are bound by the *Galateo* to participate without aliases. However, no digital identification is required (e.g. SPID, CIE). While the platform is primarily intended for the residents of Milan and their representatives, the lack of certified authentication or subsequent checks by the organizers effectively means that there are very few limitations on who can participate.

Each participant can start a discussion over whatever object of interest, by simply posting it. Other participants can comment or react to comments (rating from one to five stars). The platform is divided in many areas ('forums') dedicated to the individual municipalities of the Comune of Milan and to the individual communes of the metropolitan area of Milan. There are also dedicated forums for special themes (e.g., environment and waste, educational system, smart city) or special categories (e.g., young people engaging individually or through school projects) or projects (e.g. mapping handicapped parking space or reporting trees affected by *Takahashia japonica*).

According to the rules set in the *Galateo*, every message is previously checked by a moderator (whose name and surname are made public) who assesses whether it is compliant with the *Galateo*. In case it is unrespectful of other participants, insulting, discriminatory, off-topic or exceeds daily limits (4 comments and 2 starts of discussion per forum), the moderator does not publish it and provides the participant with a written explanation.

It is worth noting that such a previous checking is possible due to the relatively small numbers of participants and comments (at the moment 7386[119] people are registered on PartecipaMi, which means 0,62% of the population of the Comune of Milan and only 0,27% if we consider the whole metropolitan area). However, it strikes the visitor to notice that there is still somewhat activity on the platform, after 16 years since it was first created. Its bottom-up nature, partnerships with other associations and foundations[120], the capacity of organizers to foster relationships with some administrators and encourage them to take part to the debate, the gradualness of topics discussed in forums, from sub-local to broader issues, are some of the factors which have determined the platform's longevity.

However, though providing citizens with a useful tool to share their ideas and engage in constructive debates, it does not have any formal partner-

participatory institutions (popular initiative, referendum, inquiries, petitions, citizen consultations and public hearings), new ones were added: public inquiry, public debate on urban works, environment and services, participatory institutions for urban and building planning, forms of participation in individual demand public services, citizens' agreements, participatory budgeting, questions with immediate answers.

117. The Rete Civica di Milano (Milan Civic Network, RCM) was initially launched in 1994 as a university project by the Civic Informatics Laboratory at the University of Milan. Its primary objective was to provide citizens with a platform for effective and easy-to-use communication and promote active citizenship.

118. Sicurezza Stradale, in collaboration with Ciclobby, Manifesto per Milano, in collaboration with Corriere della Sera, and Cives, which was funded by the Cariplo Foundation. See more on PartecipaMi website.

119. As of 30 April 2023.

120. E.g., those which promote active citizenship in school.

ship with official institutions, thus lacking means to force them to listen to the citizens' claims and opinions – much less enforce implementation of proposals. After an issue has been raised and discussed, the organizers report it to local administrators (through e-mails at institutional addresses or informal contacts). However, these administrators are not obligated to put the proposals into practice or even to provide a response.

In sum, PartecipaMi is a useful participation tool to foster Milan's civic network through debate, citizen reporting and information gathering. Eventual listening of its proposals by institutions, through the reporting via the platforms' organizers[121], does not change its nature which remains "horizontal" in the first place. That is why it can be classified as a practice of Sharing (Level 5) according to the Framework[122].

C. MeinBerlin

As third case study of this paper we will now analyse the participatory platform of the city of Berlin, i.e. meinBerlin. Participation processes of all administrative units at State (*Land*) and local (*Bezirk*)[123] level can be realised on the platform, which serves as «one-stop participation portal»[124]. Created in 2015, this top-down platform aims at informing the citizens of Berlin of the ongoing projects of the city's administration, providing a space for sharing ideas and suggestions. The platform was built using Adhocracy, an open-source software developed by Liquid Democracy e.V., a non-profit German organisation. Publisher of the platform is the administrative staff of the Governing Mayor of Berlin (*Senatskanzlei*, Senate Chancellery) which is also responsible for placing projects on the platform[125].

The development of meinBerlin began in 2013 when the Senate Department for Urban Development and Environment (*Senatsverwaltung für Stadtentwicklung und Umwelt*) decided to digitalize legally required citizen participation processes in urban land use planning[126]. Meanwhile, the district of Treptow-Köpenick was planning an online platform for informal citizen participation processes. Under the supervision of the Senate Chancellery these two activities were merged in 2015. Thus, both legally prescribed processes and informal processes are carried out on the platform. In 2015 Berlin also adopted an eGovernment Act, which contains a declaration of intent to promote e-participation in political and administrative action, but no binding measures of actual implementation[127].

Registration is required to participate, serving the purpose of reducing the incidence of bots and trolls, which can disrupt the participation process. However, low-threshold registration requirements

121. It must be noted that the reporting of participants' ideas and claims via e-mail by PartecipaMi's organizers could be seen as a practice of 'unsolicited feedback', which is included among forms of 'listening' (Level 6) of institutions to the citizens' needs.
122. For more information on PartecipaMi as a practice of sharing, see De Cindio-Trentini 2024, § 5.
123. Berlin enjoys a particular status, being both the capital of Germany and one of its sixteen *Länder* (federated States). It divides into 12 districts (*Bezirke*). Although it is legally a State, we chose to treat it as a local experience, due to the similarities in dimension and population with the cities of Rome and Milan.
124. Pruin 2022. Currently, 44 authorities and subordinate organisations can conduct consultations on meinBerlin, including the Berlin Senate Chancellery (*Senatskanzlei*), the State Departments (ministries), the district administrations, the subordinate authorities of the districts and state-owned companies. Centralisation of all participation projects is intended to foster the integration of online citizen participation into the planning processes of those administrative units that have not yet conducted any or have conducted only a few participation processes. *Ibidem*, 213.
125. However, while the technical implementation and strategic development of the platform are centralised, it is the competent administrative units either at the state or district level that carry on the actual organisation, moderation and evaluation of the individual participation processes. See Pruin 2022, p. 214.
126. The Federal Building Code (*Baugesetzbuch*) entails a number of provisions on public participation in urban development. See Sinning 2018.
127. See Pruin 2022, p. 214.

are foreseen (email address, username, and password). On one hand, this guarantees easy access for a wide range of individuals. On the other hand, it eliminates the possibility of identity or status control, such as citizenship or residency. As of 2020, meinBerlin had slightly more than 9,000 registered users, comprising approximately only 0.31% of Berlin's population over the age of majority.

The types of participation meinBerlin allows theoretically range from participatory budgeting to public surveys, open debates, idea gathering and participation in urban land use planning. However, apparently no participatory budgeting experiences have been carried with the help of the platform yet[128] and what can be found on the meinBerlin is often solely information on participation processes, which are carried out offline, thus not representing a form of ICT-enabled joint decision making, but rather simple providing citizens with information[129]. Most of the processes carried on the platform seem to be consultations (Level 6 in the Framework): the platform offers the possibility to submit ideas or proposals, comment and evaluate those by other users, map their ideas on a map, participate in cooperative text editing, but citizens' are only able to provide feedback to the institutions on pre-established themes and projects, i.e., during formal building plan procedures[130].

D. ParteciPa

In 2011, ParteciPA (wordplay that signifies both "participate" and "take part in the public administration") was created by FormezPA[131] with the aim of improving the quality and transparency of public decisions through the on-line involvement of stakeholders (citizens, businesses and trade associations)[132]. Conceived as an open source participatory platform – inspired by social networks' operating mods – it was structured as a top-down participatory instrument available for any Italian

128. It is to note that one of the districts of Berlin (Lichtenberg) has a thirteen-years-long tradition of participatory budgeting and its own website for this purpose. Anyone can submit a proposal either directly on the website, via e-mail or in person. On the platform people can also view all proposals on a map and provide feedback (by commenting or supporting through a sort of 'like'-button) on other proposals. However, this digital feedback has no bearing on the proposal evaluation and approval process. Proposals are drafted with administrative assistance to ensure they meet specific criteria and then voted on by a citizen jury. There is no digital voting procedure, intermediate or final, that is open to all residents and city users, which differs from the blended model used for #ROMADECIDE. Thus, the Lichtenberg website appears to be entirely informational about a mostly offline participatory process.

129. Pruin 2022, p. 214. This type of content should fall under Level 4 [*information*].

130. It is to praise the effort to attain a high level of accountability and transparency about the outcome of the consultations. The FAQ section of meinBerlin clarifies that the project managers will evaluate all contributions, and detailed information about the outcome of the submitted content, including when and where the results will be published, can be found under the "Results" section. The Guidelines for citizens' participation in projects and processes of urban development (which were adopted following a two-years process between 2017 and 2019, with participation of 12 randomly selected citizens in the relevant committee, see this link) emphasize the need for accountability of administrations that coordinate citizen participation. To address this need administrations are bound to provide written public feedback regarding the results of participation, making it clear how citizens' recommendations were incorporated into the final decision, and, if not, why. Since the majority of the projects regard urban development and requalification, these guidelines are of some importance.

131. FormezPA is a recognised association with legal personality that provides service, assistance, studies and training for the modernisation of PAs. It is in-house to the Presidency of the Council (Department of Public Service) and its associated administrations. Established in 1963, it originally exercised its functions within the system of extraordinary interventions for Southern Italy. Over the years, FormezPA has undergone profound changes that have allowed it to acquire a central role in promoting innovation and strengthening administrative capacity, as foreseen by EU development policies.

132. As per the provisions of Article 9 of the CAD, see *supra* § II.

Public Administration (PA) aiming to try new ways to increase citizens and other stakeholders' engagement on specific issues.

The structure of participatory processes was outlined essentially in three phases: ideation, commentary and experiences.

- Ideation: initial thread to collect, comment, vote and aggregate user ideas on a specific topic also through surveys or questionnaires.
- Commentary: second thread to discuss rules, legislative proposals, documents, on which users can comment on individual paragraphs.
- Experiences: final space where users can create threads to share, evaluate and comment on projects carried out in the public and private sector, involving PAs in various ways.

Since 2019 ParteciPA has been modernised; still an open source and top-down participatory platform, it now utilizes the Decidim software and is currently managed by the Department of the Civil Service and the Department for Institutional Reform, both of which are overviewed by the Presidency of the Council of Ministers.

The *Decidim* open source software was initially developed by the citizens of Barcelona and allows to manage the participatory processes of a community (administration, association, party) in a single platform, in a homogeneous mode that makes participation easier. For example, one could use the platform to propose actions, comment, monitor and plan meetings in presence.

Due to its top-down nature where threads are launched exclusively by the administrations, in ParteciPA not all these features are allowed to citizens.

In order to access the platform, citizens have to log in through their profile within the public identification service, the SPID[133].

Once the citizen intervenes with a comment or a response to a survey or questionnaire, it cannot be modified or removed autonomously, but it can be erased by the admins if it doesn't comply with the community standards.

As of March 2023 there have been a total of twenty-five participatory processes on ParteciPA, but, despite the user-friendly interface, the users that actually took part in each discussion went as high as a little over one hundred.

The 2022 Digital Economy and Society Index (DESI)[134] offers some explanation: Italy is above the European average in technological integration and connectivity, but it slides third to last in EU when it comes to human capital[135]. In Italy only 46% of individuals possessed at least basic digital skills in 2021, although the percentage of people having advanced digital skills matches the EU average, and the 9.8% of ICT specialists in EU as a whole works in Italy. This numbers however are only partially a justification, since independent surveys claim that Facebook users in Italy are over 38 million.

In our opinion, the reasons for such a sporadic use of the advanced tools made available for participation cannot be examined without taking into account the political phenomenon of rising abstentionism. Even if the constant raise of abstentionism since 1979 – in Italy as well as in EU – can be considered partially physiological, compulsory voting having been abolished[136], it shows a widespread disinterest in the involvement into the democratic process[137]. Even more so when it comes to

133. See footnote 74.

134. Italy ranked 18th out of 27 EU Member States in 2022 edition of the DESI. DESI reports have been redacted by the EU Commission since 2014 in order to monitor Members' States digital progress. Each year, DESI includes country profiles which support Member States in identifying areas requiring priority action as well as thematic chapters offering a European-level analysis across key digital areas, essential for underpinning policy decisions. The DESI 2022 reports are based mainly on 2021 data and tracks the progress made in EU Member States in digital. During the COVID-19 pandemic, Member States have been increasing their digitalisation efforts. See: https://digital-strategy.ec.europa.eu/en/policies/desi

135. See DESI thematic chapter.

136. Bertoncini 2014.

137. Piermarini-Paolinelli 2022.

local elections, which in the latest turnouts have seen a decrease of affluence as well[138].

Nevertheless, digital illiteracy impacts public participation: participation platforms made available are generally less challenging in comparison to entertainment products, such as social media or streaming platforms, this user friendliness did not apparently reflect on citizens' engagement and responsiveness to public and political issues, thereby posing the higher question on whether technology should, in fact, provide a broader comprehension over complex topics, and not merely supply endless accessibility and interaction sources.

ParteciPA can be considered at level 6 of the Framework, since it allows to institutionally solicit feedback from citizens on various subjects.

E. Participation-Citoyenne

Similarly, in France the *Direction interministérielle de la transformation publique* (DITP)[139] in 2017 released the website Participation-Citoyenne.gouv.fr, with the goal of informing citizens about the open consultations – ongoing or past – launched by ministries and reporting about their implementation and more in general coordinate different participation methods. In fact, there is more integration with platforms and resources at a local level in France than what we see in ParteciPA. Every consultation is directly managed by the administration that launched it, through a specific site or platform.

Participation-Citoyenne works as a one-stop portal for participatory procedures activated by French administrations. One can search a participatory initiative on the site, find out its promoters, as well as its guarantors[140]. Once the participatory process is finished, the details on its unfolding, results and implementation are shared on Participation-Citoyenne.

Moreover, unlike within the Italian platform, not all citizens have automatic access to any concertation or consultation, after having registered on the website[141]; individuals have to apply and the administration that launched the consultation will evaluate their admittance. Contrary to what happens in ParteciPa, most of the processes are not open for anyone to join in, and evaluation is based on two criteria: the impact that the policy discussed will have on the individual[142] and the quality of contribution the citizen can give to the discussion[143].

Considering the Reports on the passed consultations, especially the ones carried out in a hybrid online-in person modality, Participation-Citoyenne apparently draws more participants than ParteciPA. Also, the exact number of participants is not explicitly divulged for every consultation, for example the latest consultation about energetic future had more than 36,000 entries online plus a wide participation in person during a regional tour of consultation. One of the latest processes that fully divulged its numbers was the national consultation on Justice in 2021, it had more than 18,000 active participants[144].

Participation-Citoyenne can be considered both on level 4 and 6 of the Framework. It is surely level 4, because it allows citizens to get informed on participatory processes, but its purpose does not end with transparency, it also solicits their feedback, tries to get them actively involved, so in this sense can be considered at level 6.

F. Comparison and evaluation: preliminary findings

In Tab. 1 we compare the 5 participatory platforms analysed, highlighting some of the most relevant characteristics, including the territorial level they express, if they are top-down or bottom-up expe-

138. A worldwide phenomenon that cannot be really tied to any political party or point of view. Chou 2017.

139. Established by décret n° 2015-1165 du 21 septembre 2015.

140. Prominent French political personalities, legal professionals and experts in the specific field on which the consultation takes place.

141. Log-in does not entail identification through a publicly sanctioned provider.

142. For example if he is a resident in one of the localities interested by the concertation, or, as in the case of the youth forum 2022, if he is under 30 years old.

143. This criteria is evaluated through the application: motivation statement, professional or academic qualification.

144. More than 21,000 active and passive participants.

riences, what kind (strong/weak) of authentication is required to access, which software is used, the level of participation in terms of number of users of the platform compared to the total population that should serve, a brief description of each participatory experience.

Following the analysis conducted in the previous paragraphs, the last column on the right side of the table shows the level these platforms express according to the Framework presented in § II. As anticipated, this classification helps to capture the profound differences of each digital democratic innovation in terms of real participation. Behind similar claims of enhancing participation and democratising democracy may hide examples of Level 4 (Transparency, i.e. partially Participation-Citoyenne), Level 5 (Sharing, i.e. PartecipaMi), Level 6 (Consultation, i.e. meinBerlin, ParteciPA, Participation-Citoyenne); proper forms of Level 7 (Democracy, #ROMADECIDE) are a rarity (and, as we will see in the following, often miss important goals).

If it is true that classifying is the first step towards evaluation, it may not be enough to assess the quality of citizen participation in these ICT-enhanced initiatives, i.e., their actual ability to democratise democracy. The comparative table also offers valuable insights into participation through participation rates, which appear to be consistently low (we will delve deeper into the problem in our Conclusions, § V). However, we do not content ourselves with these indicators and we try to address the challenge of evaluating the quality of these use-case digital democratic innovations building on two further indicators: 'meaningful participation' and 'digital deliberation'[145].

PLATFORM	LOCAL / NATIONAL	T.D./B.U.	AUTHENTICATION	SOFTWARE	USERS/ POPULATION	DESCRIPTION	LEVEL
Roma Decide	local	Top down	strong	Proprietary	0,77%	Participatory budgeting	7
PartecipaMi	local	Bottom up	weak	openDCN	0,27%	Civic network	5
Mein Berlin	local	Top down	weak	Adhocracy	0,31%	One-stop participation platform	6
ParteciPA	national	Top down	strong	Decidim	0,00%	Consultations promoted by different PAs	6
Participation Citoyenne	national	Top down	weak	Proprietary	0,00039%	Collector of consultation processes by different PAs (links and results)	4/6

Tab. 1 — *Comparative table of our five use-case participatory platforms*

145. These indicators are inspired by one of the most comprehensive frameworks for evaluating democratic innovations: Brigitte Geissel and Marko Joas's framework to evaluate Participatory Innovations, defined as «new procedures consciously and purposefully introduced with the aim of mending current democratic malaises and improving the quality of democracy» (cfr. Geissel 2013, *Introduction*, p. 9). The authors propose six indicators, starting by a) meaningful participation and b) deliberation. The other four indicators proposed are, as admitted by the authors themselves, particularly difficult to evaluate in a concrete scenario, especially with the data available. The third indicator c) 'inclusiveness of participation' (participation of all stakeholders, including minorities) poses problems of data protection (the organizers themselves often do not even ask for information about gender or income). However, when it was possible to gather information at an aggregate level, data have shown that participants are by no means a representative sample of the interested population, living mostly in inner-city districts and having a better-than-average education (see, concerning meinBerlin, Pruin

Meaningful participation indicates to what extent the participants' preferences were transformed into policies. Digital deliberation indicates the level of digitalisation of the process of thoughtful weighing of opposing arguments before taking a decision. On the background of these indicators applied to digital democratic innovations we can find, respectively, the core values of participatory democracy, on the one hand, and of deliberative theories, on the other.

Firstly, applying the criterion of 'meaningful participation' to #ROMADECIDE, there is no doubt that in a process of participatory budgeting citizens' preferences are effectively translated into policies. As mentioned, it is possible to track the state of art of the implementation of the proposals on a dedicated page on the website of Roma Capitale. The effort to be transparent and accountable is praiseworthy: 27 of the 65 projects were finalised, 11 are underway, 9 at the stage of tender, 17 still need to be designed, 1 was apparently not considered[146]. However, it must be noted that #ROMADECIDE remains insofar a one-time experience, although the special Regulation of the *Bilancio Partecipativo* mentioned in § I suggests participatory budgeting should take place "normally yearly"[147]. For many scholars if the process is not repeated over years it is not even a real example of participatory budgeting[148]. Without reaching such drastic conclusions for #ROMADECIDE, we can point out that long-term positive effects (i.e., investments in healthcare assistance and services, increased number of organisations active in the community, and decreased the infant mortality rate[149]) were registered when participatory budgeting has constant application over time. Trying to evaluate how 'deliberative' the digital process was, it must be noted that what took place on the platform was the mere posting of proposals and voting them (it was an 'hybrid' form of participatory budgeting). Of course, each municipality had to organize meetings designed to enable the discussion of proposals that they were required to present (and for which 20% of the municipality's budget was reserved). However, apart from these meetings no other online or offline spaces were institutionally foreseen for citizens to engage in dialogue and deliberation. The platform itself apparently did not

2022, p. 217). The other three indicators are: d) 'perceived legitimacy' derived by citizens' support to political institutions; e) 'effectiveness', which refers to whether the democratic innovation solved collective problems better then via decisions of political representatives (the distinction between meaningful participation and effectiveness lies in the fact that while meaningful participation promises that the *output* policies will take into account the contribute of citizens in the decision-making process, it does not necessarily guarantee that the *outcome* will be the resolution of the problem: for instance, while participatory budgeting may result in the implementation of actual public policies that reflect citizens' preferences, the desired outcome, such as improving the quality of life in a city through sustainable urban planning, may not be achieved); f) the 'enlightenment of citizens' and their 'democratic education' fostered through improvement of knowledge, tolerance, and public spiritedness.

146. As of 6 May 2023. While it is important to acknowledge the potential impact of the COVID-19 pandemic on project implementation timelines, it is also disheartening to witness the number of initiatives that continue to be held up by bureaucratic hurdles.

147. 'Normally yearly' the governing body of Roma Capitale (*Giunta Capitolina*) should indeed determine the essential characteristics of the participatory budget, including budget, destination, characteristics and limits of the proposals, timing and so on. Despite this and other programmatic provisions in the reformed Statute of Roma Capitale, the decision whether to implement participatory budgeting is therefore ultimately in the hands of the governing body.

148. Sintomer-Herzberg-Röcke-Allegretti 2012, p. 3.

149. These parameters were put in relation to long-term participatory budgeting experiences in Brasil (Cfr. Chiusi 2014, p. 159). However, it could be pointed out that those parameters relate to the outcome (and, thus, the 'effectiveness') rather than the mere output ('meaningful participation') of this participatory budgeting experience (see footnote 128). #ROMADECIDE would thus score high in 'meaningful participation', though it was a one-time experience, but shows a low level of 'effectiveness'.

have a dedicated feature for advertising self-organised meetings for discussing proposals. From this point of view, this e-participation tool did not show a high level of digitisation of the debate, and debate, where present, took place offline.

Moving on to partecipaMi, we must note that as a practice of sharing there is no direct involvement of institutions in the participatory processes, thus lowering the 'meaningfulness of participation' parameter. Voluntary engagement by politicians and city councillors on the platform could potentially improve this aspect, but it has historically been difficult to encourage such engagement. Additionally, while the organizers state they report continuously via e-mail to the relevant administrations what happens on the platform, PAs may decide not to respond.

Conversely, despite not being a cutting-edge deliberation platform[150] and frequently failing to reach a shared decision, partecipaMi's online discussions on particular topics serve as a compelling example of informed exchange of opinions and high-quality online debate. Additionally, since the online debates are public and permanently available, they constitute a common informational asset that can be accessed at any time if a particular issue becomes relevant again in the future, making them a valuable resource for future reference. [151]

Regarding MeinBerlin, having outlined that most participatory processes carried out on the platform are consultations, thus being up to the relevant PAs whether to take citizens' preferences in consideration, participation 'meaningfulness' appears rather low. However, as already mentioned at the end of § IV C, there seem to be a great effort in transparency and accountability: PAs must provide feedback to the citizens' opinions and proposals, especially when they decided not to incorporate citizens' recommendations in the final decision.

Furthermore, meinBerlin appears to be lacking in terms of digital deliberation. Even leaving actual decision-making out of focus and considering deliberation in a broader sense as the exchange of thoughtful opinions, it seems that this mostly happens offline during institutional meetings. Additionally, citizens' online comments on urban planning proposals are evaluated as individual contributions by public authorities rather than being collectively discussed among participants.

Considering now ParteciPA and Participation-Citoyenne, in both cases the Administrations that launched the consultations are obliged to divulgate the numbers (active and passive participants, comments, discussions etc.), content and impact of consultations. However, although results are to be taken into account by the relevant PAs (or the parliament, in some cases) the meaningfulness of participation remains ultimately in the hands of the promoting institutions.

Concerning deliberation, the agglomerative nature of both platforms, allowing PAs to organize the consultations as they see fit, prevents them from being evaluated as a whole. Depending on the specific participatory process, there could be more or less deliberation. For example, the latest climate consultation in France had moments of deliberation both in-person and online.

150. A field of research on platforms for online deliberation is experimenting ways to scaling up online deliberation for complex problems. Simply moving conversations into the digital world leads to a simple exchange of text and speech online, producing large disorganised and often low-quality comment piles. Such conversational tools also create perverse incentives to polarisation and extremisation, on the one hand, and self-censoring, on the other. The approach based on deliberation mapping seeks to transcend those limitations, allowing quick and efficient problem-solving: all contributions appear as points in that part of the map where they logically belong, e.g. all answers to a particular question under that question (an example of that is the e-deliberation platform Deliberatorium, cfr. Klein 2022; see also Klein-Convertino 2014, p. 40 ff.; another example of digital deliberation platform is COLLAGREE, cfr. Yang-Gu-Ito-Yang 2021, pp. 4762 ff.). Many streams of research are also focusing on the possibility to use Natural Language Processing for (semi-)automatic moderation of online deliberation, providing real-time visualisation of argument maps, detection of fallacies in reasoning, hate speech detection, motivating more argumentation highlighting parts of an argument that are a good target for attack, fact checking and source identification and so on: see Vecchi-Falk-Jundi-Lapesa 2021.

151. One may ask if the quality of the debate depends on the particular engagement and level of education of participants, other than on the relatively small number of participants in a conversation. Would then problems arise if we scale up participation and make it more inclusive?

V. Conclusions

As argued in the previous paragraph, it is indeed challenging to achieve a qualitative evaluation of e-participation through platforms. Nevertheless, from an observation of the numbers at Tab. 1 it can be said that specific platforms for e-participation still draw small attention from their main target: citizens. Even in relatively successful instances like PartecipaMi or Participation-Citoyenne, with many entries and contributions from users, the overall percentage of participants is still quite low. In the past decade many authors have argued that the best antidocte to the democratic crises – abstentionism, populism and so on – could only be an increased involvement of citizens throught participatory instruments and an overall better informed electorate. Often, the same authors would also suggest that these two elements would be easier to achieve thanks to technological development[152]. One of the observations we would like to underline, in our conclusion, is that although the technological development can open new opportunities, the mere presence of useful tools is not enough to overcome democratic crises, if the *démos* stays idly by. It is true that the proliferation of institutional platforms for consultation and participation denotes that a new understanding of the importance of participation from institutional players has been undoubtly achieved, but there is still a long way ahead.

Regarding Italy, we already saw in § IV D speaking of DESI 2022 that the lack in digital participation may be attributed, at least partially, to the lack of digital knowledge. Among the four indicators of the DESI (human capital, connectivity, integration of digital technology and digital public services) the greatest struggle for Italy is represented by the human capital: still more than half of Italian population does not have at least basic digital skills. Still, there is a great gap between a maximum of 150 users on ParteciPA and 38 million Italian users on Facebook. Blaming the digital divide does not appear appropriate. In Germany only around 50% of internet users possesses at least basic digital skills[153]. But the numbers are still low when we consider France, where almost the entire population has access to internet and almost 80% of internet users has at least basic digital skills. Furthermore, these percentages cannot be attributed to the mere ignorance of the e-participation platforms' existence or to the citizens' lack of commitment.

Our shared impression is that citizens either are not interested in themes on which they are called upon, or they do not know that they can participate in discussions on themes that they are interested in. It has been proposed to try to use directly the most popular social networks to catalyze citizen participation. It could be an opportunity to draw citizens attention to the existence of platforms and specific consultations. After all, Public Administrations have once already used Social Networks to redirect users on official channels, campaigning against fake news on Covid-19 pandemic or to draw people's attention on the importance of vaccines.

Beyond the participation rates, which could benefit from a larger-scale publicity of these initiatives, the low percentages of engaged citizens can also be attributed to the time-consuming nature of participation. In the early sections of the paper we questioned to what extent digital democratic innovations could serve as an antidote to abstentionism. The case studies show that people are unlikely to dedicate substantial time to participation platforms unless a specific initiative deeply interests them, mirroring – and not changing – their reluctance to invest time in getting informed and voting. Hence, with such low rates of participation, the contribution of these platforms to "input-oriented" democratic legitimacy is notably limited[154].

Nevertheless, digital democratic innovations could still be valuable in gaining "output-oriented" legitimacy.[155] In other words, although we do not exclude that digital democratic innovations can ulti-

152. Zarkadakis 2020, p. 79 ff.

153. Source: DESI thematic chapter.

154. Where political choices are assessed against the extent to which the individuals subject to these decisions were involved in their formulation directly.

155. When political choices are assessed against the extent to which they effectively promote the common welfare of a community, the well-being of the people, see: Strebel-Kübler-Marcinkowski 2019, p. 491.

mately enhance the 'perception'[156] of democratic legitimacy, the main contribution of the platforms for participation may not lie in their ability to fulfill the desire to participate or be heard, but in the production of more satisfactory policies for the community.

In conclusion, it seems that the mere proliferation of technological tools and participation platforms does not necessarily imply an improvement in commitment, a better understanding of political themes or, for that matter, a higher quality of the public discourse. The exceptionally rapid growth of civil society's technical proclivity in using devices and digital tools did not, by far, fulfill the utopian dreams of the inherent value of 'connection,' per se, fostered by social networks' founders. It is known that the world wide web and especially social networks are daily enslaved by illiberal regimes' liberticidal practices, such as censorship and surveillance of citizens. However, within the abovementioned EU regulatory context, social networks and platforms serve as invaluable sources for real-time feedback and diverse perspectives, enabling enhanced citizen engagement and data-driven policy formulation.[157] Nonetheless, addressing challenges such as data privacy and misinformation is imperative to uphold principles of inclusivity and accountability in governance. The original idea that connection among individuals, as such, would have benefitted society in spreading positive thoughts and marginalizing conspiracy theories, racism etc., simply did not materialise.

Finally, the institutionalized use of social platforms to catalize attention and providing access to public forums indirectly invested with small amount of decision-making has the potential to draw proper attention to common problems and help institutions meeting the citizens' needs. Time, public investments and further research on the positive externalities of digital democratic innovations are certainly required to fully realise their potential and enhance their impact.

The paper is the result of the joint work of the two Authors. However, §§ I, II and IV A, B C and F can be attributed to Teresa Balduzzi, §§, III, IV D, E and V to Livia Siclari. Translations of foreign contributions and regulations have been cured by the Authors. The paper has been developed as part of the International Research Network (IRN) "e-DELIB Democracy and Liberties in the Digital Age: Towards E-Democracy by Law 2021-2025". The findings of this study are presently undergoing the publication process on e-DELIB's blog.

Bibliography

U. Allegretti (2011), *Il cammino accidentato di un principio costituzionale: quarantana anni di pratiche partecipative in Italia*, in "Rivista AIC", 2011, n. 1

U. Allegretti (2010), *Democrazia partecipativa: un contributo alla democratizzazione della democrazia*, in Id. (ed.), "Democrazia partecipativa: esperienze e prospettive in Italia e in Europa", Firenze University Press, 2010

U. Allegretti (2008), *Democrazia partecipativa e processi di democratizzazione*, in "Democrazia e diritto", 2008, n. 2

U. Allegretti (2006), *Basi giuridiche della democrazia partecipativa*, in "Democrazia e diritto", 2006, n. 3

S.R. Arnstein (1969), *A ladder of citizen participation*, in "Journal of the American Institute of planners", vol. 35, 1969, n. 4

G. Balduzzi, D. Servetti (2017), *Effettività del principio democratico e democrazia deliberativa: il percorso di istituzionalizzazione di una sperimentazione locale*, in "Il Politico", vol. 82, 2017, n. 1

156. 'Perceived legitimacy' is indeed one of the indicators chosen by Geissel and Joas's framework to evaluate Participatory Innovations, see footnote 134.

157. See Cardone 2021, p. 15.

R. Beacon (2021), *What is the State of Debate on Digital Democracy?*, Tony Blair Institute for Global Change, 2021

Y. Bertoncini (2014), *European Elections: the abstention trap*, Policy Paper 110, Notre Europe, Jacques Delors Insitute, 2014

R. Bifulco (2017), *Democrazia deliberative e principio di realtà*, in "Federalismi.it", 2017, n. 1

R. Bifulco (2009), *Democrazia deliberativa e democrazia partecipativa*, in "Astrid Rassegna", 2009

R. Bifulco (2009), *Democrazia deliberativa, partecipativa e rappresentativa: tre diverse forme di democrazia?*, in U. Allegretti (ed.), "Democrazia partecipativa : esperienze e prospettive in Italia e in Europa", Firenze University Press, 2010

L. Bobbio (2006), *Dilemmi della democrazia partecipativa*, in "Democrazia e Diritto", 2006, n. 4

J. Bohman (2004), *Realizing Deliberative Democracy as a Mode of Inquiry: Pragmatism, Social Facts, and Normative Theory*, in "The Journal of Speculative Philosophy", vol. 18, 2004, n. 1

G. Bosetti, S. Maffettone (eds.) (2004), *Democrazia deliberativa: cosa è*, Luiss University Press, 2004

A. Cardone (2021), *Decisione algoritmica vs. decisione politica? AI, legge, democrazia*, Editoriale Scientifica, 2021

E. Carloni (2019), *Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni*, in "Diritto pubblico", 2019, n. 2

J. Chevallier (2011), *Délibération et participation*, in Conseil d'État, "Rapport public", 2011

J. Chevallier (2006), *La démocratie délibérative: mythe et réalité*, in "Politiques, communication et technologies. Mélanges en hommage à Lucien Sfez," Presses universitaires de France, 2006

F. Chiusi (2014), *Critica della democrazia digitale – La politica 2.0 alla prova dei fatti*, Codice edizioni, 2014

M. Chou (2017), *Political knowledge and paradox of voting*, Cornell Policy Review, 2017

B. Constant (1992), *Discorso sulla libertà degli antichi paragonata a quella dei moderni*, Ed. Riuniti, 2012

M. Crozier, S.P. Huntington, J. Watanuki (1975), *The Crisis of Democracy. Report on the Governability of Democracies to the Trilateral Commission*, New York University Press, 1975

A. D'Atena (1998), *Il principio democratico nel sistema dei principi costituzionali*, in A. D'Atena, E. Lanzillotta (ed.), "Alle radici della democrazia. Dalla Polis al dibattito costituzionale contemporaneo", Carocci, 1998

F. De Cindio, A. Trentini (2024), *Cittadinanza Digitale e Tecnocivismo*. Volume II, 2024, *forthcoming*

F. De Cindio, A. Trentini (2014), *A layered architecture to model digital citizenship rights and opportunities*, in "Conference for E-Democracy and Open Government", 2014, p. 403 ff.

F. De Cindio, L. Sonnante, A. Trentini (2012), *Cittadinanza Digitale: un arcobaleno di diritti e opportunità*, in "Mondo Digitale", 2012, n. 42

Department of Economic and Social Affairs of the United Nations Secretariat (2005), *Citizen Participation and Pro-poor Budgeting*, 2005

M. Di Folco (2023), *Partecipazione democratica e diritti di libertà*, in D. Morana (ed.), "I diritti costituzionali in divenire", II ed., Editoriale Scientifica, 2023, p. 291 ff.

N. Dias (ed.) (2018), *Hope for Democracy. 30 Years of Participatory Budgeting Worldwide*, Oficina, 2018

J.S. Fishkin, R.C. Luskin (2005), *Experimenting with a Democratic deal: Deliberative Polling and Public Opinion*, in "Acta Politica", vol. 40, 2005

A. Floridi (2020), *Habermas e la democrazia deliberativa*, in "Quaderni di Teoria Sociale", 2020, n. 1-2, p. 341

A. Floridia (2017), *Un'idea deliberativa della democrazia*, il Mulino, 2017

G. Geissel (2013), *Introduction: On the Evaluation of Participatory Innovations - A Preliminary Framework*, in B. Geissel, M. Joas (eds.), "Participatory Democratic Innovations in Europe: Improving the Quality of Democracy?", Barbara Budrich Verlag, 2013

G. Gometz (2017), *Democrazia elettronica. Teoria e tecniche*, Edizioni ETS, 2017

L.L. Grossman (1996), *The Electronic Republic: Reshaping Democracy in the Information Age*, Penguin Books, 1996

S. Guerard (2007), *La démocratie locale, une approche de droit comparé*, in F. Robbe (ed.), "La démocratie participative", L'Harmattan, 2007

J.P. Horsley (2009), *Public Participation in the People's Republica: Developing a More Participatory Governance Model in China*, in "Yale Law Review", 2009

M. Klein (2022), *Crowd-Scale Deliberation For Complex Problems: A Progress Report*, preprint published in March 2022 on researchgate.net

M. Klein, G. Convertino (2014), *An Embarrassment of Riches. A critical review of open innovation systems*, in "Communications of the ACM", vol. 57, 2014, n. 11

M. Luciani (2005), *Art. 75 Cost.*, in G. Branca, A. Pizzorusso (eds.), "Commentario della Costituzione", Zanichelli, 2005

Y. Mansillon (2006), *L'esperienza del Débat Public in Francia*, in "Democrazia e Diritto", 2006, n. 3

F. Martines (2023), *Piattaforme digitali dell'Unione europea e strumenti di democrazia partecipativa*, in "Osservatorio sulle fonti", 2023, n. 2

J. Mendes (2011), *Participation and the role of law after Lisbon: a legal view on article 11 TEU*, in "Common Market Law Review", vol. 48, 2011, n. 6

A. Morelli (2015), *Le trasformazioni del principio democratico*, in "Consulta online", 2015, n. 1

K. Newton (2012), *Curing the democratic malaise with democratic innovations*, in B. Geissel, K. Newton (eds.), "Evaluating Democratic Innovations – Curing the democratic malaise?", Routledge, 2012

OECD, *Citizens as Partners: Information, Consultation and Public Participation in Policy-Making*, 2001

C. Pateman (2012), *Participatory Democracy Revisited*, in "Perspectives on Politics", vol. 10, 2012, n. 1

G. Pepe (2020), *Il modello della democrazia partecipativa tra aspetti teorici e profili applicativi: un'analisi comparata*, Cedam, 2020

N. Pettinari (2019), *Gli strumenti di democrazia partecipativa nelle costituzioni e la partecipazione ai processi costituenti*, in "Federalismi.it", 2019, n. 15

M. Picchi (2012), *Il diritto di partecipazione*, Giuffrè, 2012

M. Piermarini, P. Paolinelli, (2022), *Astensionismo elettorale e metamorfosi della democrazia liberale*, in "Critica sociologica", 2022, n. 2

F. Politi (2021), *Democrazia rappresentativa versus democrazia diretta. Riflessioni preliminari su democrazia parlamentare, democrazia partecipativa e democrazia deliberativa*, in "dirittifondamentali.it", 2021, n. 1

A. Pruin (2022), *How organizational factors shape e-participation: Lessons from the German one-stop participation portal* meinBerlin, in T. Randma-Liiv, V. Lember (eds.), "Engaging Citizens in Policy Making: e-Participation Practices in Europe", Edward Elgar Publishing, 2022

E.C. Raffiotta (2023), *Dalla* self-regulation *alla* over-regulation *in ambito digitale: come (e perché) di un necessario cambio di prospettiva*, in "Osservatorio sulle fonti", 2023, n. 2

S. Rodotà (1997), *Tecnopolitica: La democrazia e le nuove tecnologie della comunicazione*, Laterza, 1997

P. Rosanvallon (2006), *La contre-démocratie. La politique à l'age de la défiance*, Paris, 2006

S. Rose-Ackerman, T. Perroud, (2013), *Policymaking and public law in France: public participation, agency independence and impact assessment*, in "Columbia Journal of European Law", vol. 19, 2013, n. 2

D. Rousseau (2020), *La démocratie continue: fondements constitutionnels et institutions d'une action continuelle des citoyens*, in "Confluence des droits", 2020, n. 2

J. Schumpeter (1976), *Capitalism, Socialism and Democracy*, Routledge, 1976

L.G. Sciannella (2020), *Il principio di partecipazione popolare nella nuova costituzione cubana*, in "DPCE Online", vol. 42, 2020, n. 1

H. Sinning (2018), *Öffentlichkeitsbeteiligung*, in "Handwörterbuch der Stadt- und Raumentwicklung", ARL, 2018, p. 1655 ff.

D. Siclari (2009), *La democrazia partecipativa nell'ordinamento comunitario: sviluppi attuali e prospettive*, in "Amministrazione in Cammino", 18 novembre 2009

Y. Sintomer, C. Herzberg, A. Röcke, G. Allegretti (2012), *Transnational Models of Citizen Participation: The Case of Participatory Budgeting*, in "Journal of Public Deliberation", vol. 8, 2012, n. 2

G. Smith (2009), *Democratic innovations: designing institutions for citizen participation*, Cambridge University Press, 2009

M. Sorice (2021), *Partecipazione disconnessa – Innovazione democratica e illusione digitale al tempo del neoliberismo*, Carocci editore, 2021

M. Sorice (2020), *Democratic Innovation*, in P. Harris et al. (eds.), "The Palgrave Encyclopedia of Interest Groups, Lobbying and Public Affairs", Springer, 2020

M.A. Strebel, D. Kübler, F. Marcinkowski (2019), *The importance of input and output legitimacy in democratic governance: Evidence from a population-based survey experiment in four West European countries*, in "European Journal of Political Research", vol. 58, 2019, n. 2

G. Trenta (2022), *La democrazia partecipativa in Italia: un viaggio ancora in itinere*, in "Democrazia e diritto", 2022, n. 1

M. Trettel (2020), *La democrazia partecipativa negli ordinamenti composti: studio di diritto comparato sull'incidenza della tradizione giuridica nelle democratic innovations*, in "Collana del Dipartimento di Scienze Giuridiche dell'Università di Verona", Edizioni Scientifiche Italiane, 2020

A. Trentini, G. Biscuolo, A. Rossi (2020), *Cittadinanza digitale e tecnocivismo*, Ledizioni, 2020

M. Tushet (2016), *New Institutional Mechanisms for Making Constitutional law*, in T. Bustamante, B. Gonçalves Fernandes (eds.), "Democratizing Constitutional Law. Perspectives on Legal Theory and the Legitimacy of Constitutionalism", Springer, 2016

N. Urbinati (2015), *Response to Elizabeth Beaumont's review of* Democracy Disfigured: Opinion, Truth, and the People, in "Perspectives on Politics", vol. 13, 2015, n. 2, p. 475 ff.

A. Valastro (2010), *Partecipazione, politiche pubbliche, diritti*, in Id. (ed.), "Le regole della democrazia partecipativa", Jovene, 2010

A. Van Lang (2014), *Le principe de participation: un succès inattendu*, in "Le conseil costitutionnel et l'environnement, nouveaux cahiers du conseil constitutionnel", 2014, n. 43

E.M. Vecchi, N. Falk, I. Jundi, G. Lapesa (2021), *Towards Argument Mining for Social Good: A Survey*, in C. Zong, F. Xia, W. Li, R. Navigli (eds.), "Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing", 2021, p. 1338 ff.

Y. Vilain (2010), *La démocratie participative dans un cadre fédéral: l'expérience Allemande*, in U. Allegretti (ed.), "Democrazia partecipativa: esperienze e prospettive in Italia e in Europa", Firenze University Press, 2010

P. Villaschi (2022), *E-democracy e rappresentanza politica*, PhD thesis, University of Milano Statale, 2022

C. Yang, W. Gu, T. Ito, X. Yang (2021), *Machine learning-based consensus decision-making support for crowd-scale deliberation*, in "Applied Intelligence", vol. 51, 2021, n. 7

G. Zarkadakis (2020), *Cyber Republic. Reinventing Democracy in the Age of Intelligent Machines*, MIT Press, 2020

M. Zinzi (2021), *La democrazia partecipativa alla prova dei presidenzialismi in America Latina*, in "DPCE Online", vol. 50, 2021

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0155 • articolo sottoposto a peer review • pubblicato in anteprima il 6 giu. 2024

PIETRO FALLETTA – ANNALISA MARSANO

Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR

La pervasività dei sistemi di intelligenza artificiale e il relativo impatto in termini di protezione dei dati personali impongono una profonda riflessione sulle recenti scelte normative del legislatore europeo e, in prospettiva, di quello nazionale. In questo senso, il contributo delinea, in primo luogo, l'attuale quadro legislativo europeo in materia di dati e IA, sullo scenario della complessa dimensione geopolitica in materia. Muovendo da queste premesse, il lavoro traccia un'analisi in chiave sistemica del Regolamento europeo sull'intelligenza artificiale (c.d. "AI Act"), evidenziando luci ed ombre del complesso rapporto con il Reg. (UE) n. 2016/679 ("GDPR") e identificando analogie e differenze tra i due atti normativi. Il contributo analizza, quindi, in ottica comparata, il sistema sanzionatorio e l'apparato di governance definiti dall'AI Act, focalizzandosi sulla delicata scelta di un'autorità di controllo nazionale per regolare l'intelligenza artificiale in Italia. Infine, gli autori formulano alcune riflessioni conclusive sui principali nodi tematici emersi nel corso della trattazione e propongono una prospettiva *de iure condendo* alla luce dell'analisi svolta.

AI Act – Intelligenza artificiale – Unione europea – Privacy – GDPR – Protezione dei dati personali

Artificial intelligence and data protection: the interplay between the European Artificial Intelligence Regulation and the GDPR

The widespread use of artificial intelligence systems and its impact on personal data protection calls for a thorough investigation of the regulatory governance adopted in this field by the European lawmaker and, in perspective, by the national one. In this sense, this paper first outlines the current European legislative framework on data and artificial intelligence, also tackling the related geopolitical dimension of the issue. The work then draws a systemic analysis of the recently approved European Regulation on Artificial Intelligence (so-called "AI Act"), showing lights and shadows of the complex interplay with (EU) Reg. no. 2016/679 ("GDPR") and identifying similarities and differences between the two regulatory acts. The paper goes on to examine, from a comparative perspective, the sanctioning system and the governance framework defined by the AI Act, focusing on the difficult choice of a national supervisory authority to regulate artificial intelligence in Italy. Finally, the authors provide some closing remarks on the most significant challenges raised in the context of the paper and propose some *de iure condendo* perspectives in the light of the studies carried out on the matter.

AI Act – Artificial Intelligence – European Union – Privacy – GDPR – Data protection

Pietro Falletta è ricercatore di Diritto amministrativo presso l'Università dell'Insubria; Annalisa Marsano è funzionario giuridico presso l'Autorità garante per la protezione dei dati personali (la partecipazione a questa attività è a titolo personale). Il presente contributo è frutto della piena condivisione di idee ed opinioni tra gli Autori. La stesura dei paragrafi 1 e 2 si deve ad Annalisa Marsano, quella dei paragrafi 3 e 4 a Pietro Falletta. Il paragrafo 5 è l'esito di una stesura condivisa.

1. Dalla strategia europea sui dati al Regolamento europeo sull'intelligenza artificiale

L'uso sempre più frequente di strumenti tecnologici supportati da sistemi di intelligenza artificiale ha profondamente innovato le relazioni umane, così come le metodologie di apprendimento e le modalità di azione del decisore pubblico[1]. In tal senso, il ricorso a strumenti di IA rappresenta una delle maggiori sfide per l'evoluzione degli strumenti di regolazione, sia per l'estrema varietà di soluzioni possibili, sia in ragione dei numerosi rischi che l'applicazione di queste tecnologie comporta[2].

Il fenomeno si colloca nell'ambito di un preciso quadro normativo europeo, che prende le mosse dalla c.d. Strategia europea sui dati 2030, varata dalla Commissione europea nel 2020[3] con l'intento di realizzare un unico sistema normativo applicabile in tutta Europa, atto a disciplinare l'economia dei dati, nonché a prevenire rischi e abusi derivanti dalla posizione dominante delle grandi piattaforme online. Le scelte del legislatore europeo al centro della Strategia riguardano, *inter alia*, la disponibilità, l'interoperabilità e la condivisione dei dati, una maggior chiarezza sulle facoltà di utilizzo dei dati stessi, la governance dei processi, la creazione di spazi comuni europei.

La Strategia europea dev'essere, quindi, interpretata come lo strumento attraverso cui l'Unione europea si è impegnata nell'avviare una concreta azione legislativa avente ad oggetto l'istituzione di un mercato unico europeo dei dati conforme ai principi su cui si fonda l'Ue.

Ciò rende evidente come l'ordinamento giuridico europeo, dopo aver formalmente riconosciuto il diritto alla protezione dei dati personali attraverso l'art. 8 della Carta dei diritti fondamentali dell'Ue, giunga ora ad incoraggiare il mercato dei dati (personali e non), con il precipuo scopo di impedire che le imprese dell'Unione possano perdere competitività dinanzi alle logiche proprietarie tipiche dei mercati extra-europei[4]. Le riflessioni in merito alla Strategia europea sul digitale e sull'intelligenza artificiale devono muovere, dunque, dalla concezione dei dati quale nuova valuta[5] e oggetto di scambio nel mercato digitale, elemento necessario per comprendere la *ratio* seguita dal legislatore europeo nel disciplinare la materia[6]. In questo senso, nella perenne esigenza di equilibrio tra il perseguimento della competitività del mercato europeo e la tutela dei principi fondamentali della persona, emerge la rilevanza, anche patrimoniale, dei dati.

1. In tal senso, cfr. van den Hoven van Genderen 2017.
2. Ciaralli 2023, pp. 41-42.
3. Commissione europea, *Una strategia europea per i dati*, COM (2020)66, 19 febbraio 2020.
4. Bravo 2021, pp. 200-202.
5. Eggers-Hamill-Ali 2013.
6. Peluso 2023.

Questo obiettivo – ancora oggi al centro dell'impegno delle istituzioni europee – viene perseguito attraverso un pacchetto di norme che regolano il fenomeno del mercato unico dei dati sotto diversi aspetti, tra di loro interconnessi:

- *Data Governance Act*[7]: volto ad individuare processi e strutture per favorire la disponibilità dei dati (personali e non) tramite il riutilizzo dei dati della PA e la condivisione dei dati tra imprese attraverso gli *European Data Spaces*;
- *Data Act*[8]: volto ad integrare il *Data Governance Act*, chiarendo chi e a quali condizioni possa creare valore dai dati;
- *Digital Services Act*[9]: volto a proteggere lo spazio digitale dalla diffusione di beni, contenuti e servizi illegali e garantire la protezione dei diritti fondamentali degli utenti;
- *Digital Markets Act*[10]: volto a contrastare gli abusi di mercato delle grandi piattaforme digitali in Europa e finalizzato a limitare gli squilibri economici e le pratiche commerciali sleali dei *Gatekeeper* (gestori di servizi digitali);
- *Artificial Intelligence Act*: volto a promuovere la diffusione di un'IA affidabile e garantire un livello elevato di protezione dei diritti fondamentali dell'individuo, sostenendo nel contempo l'innovazione e il miglioramento del mercato interno[11].

Ognuno degli atti sopra riportati presenta la forma di regolamento e, pertanto, è anzitutto indirizzato ad una piena armonizzazione delle relative discipline[12].

In tale contesto, il legislatore europeo è intervenuto, per primo a livello mondiale, a disciplinare l'intelligenza artificiale, dando vita al Regolamento proposto dalla Commissione europea nell'aprile 2021 e finalizzato a stabilire regole armonizzate in materia di IA (di seguito, il "Regolamento" o "AI Act")[13].

Il Regolamento persegue il duplice obiettivo del Libro bianco sull'intelligenza artificiale[14] di promuovere l'adozione dell'IA ed affrontare i rischi associati all'utilizzo di tale tecnologia, allo scopo di sviluppare un ecosistema di fiducia attraverso un quadro giuridico per un'IA affidabile[15].

In via generale, il Regolamento prevede che la disciplina europea dell'IA sia equilibrata e proporzionata, evitando di limitare eccessivamente lo sviluppo delle nuove tecnologie ed evidenziando allo stesso tempo i rischi che possono derivare da determinati utilizzi dei sistemi di intelligenza artificiale[16]. Il quadro normativo relativo all'intelligenza artificiale dovrà essere, pertanto, in grado di assicurare che tali sistemi siano utilizzati nel rispetto dei valori dell'Unione europea e del diritto attualmente vigente, nonché garantire che

7. Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (regolamento sulla governance dei dati).
8. Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati).
9. 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).
10. Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali).
11. Finocchiaro-Pollicino 2022.
12. Cerrina Feroni 2022.
13. Cfr. 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 come successivamente modificata nel corso della procedura 2021/0106 (COD) conclusa con l'approvazione del Parlamento europeo.
14. Sul punto, cfr. Pacileo 2022, pp. 305 e 306.
15. Commissione europea, *Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia* (COM(2020) 65), 19 febbraio 2020.
16. Al riguardo, si veda, tra gli altri, Scherer 2016, p. 365.

i cittadini europei possano beneficiare delle nuove tecnologie di IA senza rinunciare ai valori e i principi che caratterizzano il sistema giuridico comune.

Una riflessione organica sulla regolamentazione della complessa materia dell'intelligenza artificiale richiede anzitutto una definizione, non certo agevole, dell'oggetto in questione[17], specie in un'ottica di correlazione con il fenomeno giuridico[18]. Al riguardo, occorre, anzitutto, domandarsi se fosse opportuno per il legislatore adottare un approccio diretto a disciplinare l'intelligenza artificiale nel suo complesso o, piuttosto, regolare le applicazioni dell'intelligenza artificiale in singoli settori o materie. La prima opzione è proprio quella percorsa dall'AI Act che ha, infatti, un approccio normativo orizzontale e si basa su una nozione molto estesa di intelligenza artificiale. Nello specifico, l'art. 3 del Regolamento definisce un sistema di IA 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»[19].

Il Regolamento include, dunque, nel concetto di intelligenza artificiale quei sistemi che, per obiettivi espliciti o impliciti, deducono, dagli input ricevuti, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali, restando invece esclusi i software di natura meno complessa, nonché i sistemi di IA utilizzati esclusivamente per scopi militari, di difesa, di ricerca e innovazione, ovvero per usi non professionali[20].

Tale definizione – in linea con quella proposta in ambito OCSE[21] – appare volutamente generica ed ampia, in modo da risultare quanto più possibile neutrale e così mitigare il pericolo di una rapida obsolescenza della normativa.

La scelta del regolatore europeo di adottare un approccio normativo orizzontale ha anche uno specifico peso geopolitico nello scacchiere internazionale. A ben vedere, come si evince dalla lettura della relazione introduttiva al Regolamento, l'interesse primario dell'Ue è quello di «tutelare la sovranità digitale dell'Unione e sfruttare gli strumenti e i poteri di regolamentazione di quest'ultima per plasmare regole e norme di portata globale». Nel panorama geopolitico attuale, quindi, la strategia dell'Unione consiste, non soltanto, nell'imporsi come leader nella produzione normativa[22], ma anche nel rendere il modello europeo un riferimento globale atto ad essere implementato in tutto il resto del mondo[23], come già accaduto in passato con la normativa sulla protezione dei dati contenuta nel Regolamento (UE) n. 2016/679 ("GDPR") (si parla in questo caso di "effetto Bruxelles")[24].

In ottica comparata, è utile infatti rammentare che il Regolamento in esame si pone essenzialmente all'interno di un contesto internazionale caratterizzato dall'assenza di una disciplina organica in materia[25]. Per questa via, v'è da considerare che i principali *competitor* su scala mondiale nel settore dell'intelligenza artificiale, ossia Cina e Stati Uniti, seppure già dotati di una regolazione in materia in grado di fungere da mezzo attraverso cui

17. Sul punto, cfr. Floridi-Cowls 2019.
18. Finocchiaro 2022, pp. 1085-1087.
19. Art. 3, n. 1 Regolamento Ue sull'intelligenza artificiale.
20. Per un'analisi definitoria del concetto di intelligenza artificiale si veda, *inter alia*, Pagallo 2017.
21. «Machinebased system that can, for a given set of humandefined objectives, make predictions, recommendations or decisions influencing real or virtual environments. It uses machine and/or humanbased inputs to perceive real and/or virtual environments; abstract such perceptions into models (in an automated manner e.g. with ML or manually); and use model inference to formulate options for information or action. AI systems are designed to operate with varying levels of autonomy», in OECD 2019.
22. In tal senso Veale-Matus-Gorwa 2023, p. 263.
23. Resta 2022, pp. 328 e 329.
24. Si veda al riguardo Bradford 2021.
25. Casonato-Fasan-Penasa 2022, p. 178.

promuovere e favorire lo sviluppo dell'IA, presentano, tuttavia, normative frammentate e per certi versi lacunose[26]. Da un lato, negli USA[27], la strategia prescelta sembrerebbe prediligere un approccio normativo soft, dettato dal timore che un eccessivo rigore regolatorio possa impedire il pieno sviluppo dell'IA[28]; dall'altro, la Cina ha inaugurato un quadro legislativo autoritario volto a promuovere un elevato sviluppo economico dell'IA ma contraddistinto da numerose lacune in termini di protezione dei dati personali[29] e da una quasi totale mancanza di trasparenza informativa[30].

D'altro canto, il limite tecnico-giuridico da riconoscere rispetto all'approccio regolatorio scelto dal legislatore europeo è rinvenibile nel fatto che le norme del Regolamento non risolvono specifici problemi né colmano precise lacune dell'ordinamento, ma trovano applicazione rispetto a qualsiasi settore della società civile, dall'ambito sanitario a quello finanziario.

Quanto all'ambito di applicazione soggettiva dell'AI Act, rileva in primo luogo la natura extra-territoriale della nuova regolamentazione. Infatti, il Regolamento si applicherà anche nei confronti dei soggetti e delle organizzazioni extra-europee, sia nel caso in cui questi abbiano uno stabilimento all'interno dell'Unione europea, sia nell'ipotesi in cui essi – pur in assenza di uno stabilimento – offrano beni o servizi nel mercato unico[31]. Più nel dettaglio, i destinatari di questo Regolamento sono prevalentemente fornitori ("*provider*") ed utilizzatori ("*deployer*") di sistemi di IA, seguiti poi da: importatori e distributori; produttori di prodotti che immettono sul mercato o mettono in servizio un sistema di IA insieme al loro prodotto e con il loro nome o marchio; rappresentanti autorizzati di fornitori che non sono stabiliti in Ue; persone interessate che si trovano nell'Unione europea.

In relazione ai principali destinatari dell'AI Act, è bene tenere presente che i fornitori – persone fisiche o giuridiche – sono coloro che sviluppano o fanno sviluppare un sistema di IA e che lo immettono poi sul mercato o in servizio[32], mentre gli utilizzatori sono coloro che utilizzano i sistemi di intelligenza artificiale. L'interazione tra fornitori ed utilizzatori costituisce il nodo centrale della ripartizione delle responsabilità nell'ambito del Regolamento. Si noti che, nell'ambito di questa relazione, l'utilizzatore non è soltanto la persona fisica che si rapporta con l'IA per ricevere un servizio, ma «persona fisica o giuridica, autorità pubblica, agenzia o 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»[33]. Conseguentemente, le società che non hanno come business quello di sviluppare o vendere tecnologia basata sull'intelligenza artificiale vanno considerate alla stregua di utilizzatori.

In relazione all'approccio adottato, il Regolamento ricorre al c.d. *risk-based approach* per classificare e categorizzare i principali sistemi di IA[34] in uso secondo una struttura piramidale fondata su quattro distinti livelli di rischio determinati dall'uso di un dato sistema: (i) rischio inaccettabile; (ii) rischio alto; (iii) rischio basso o minimo; (iv) rischio specifico per la trasparenza. L'approccio *risk-based* introduce restrizioni ed obblighi a cui attenersi a seconda del grado di rischio che una determinata applicazione può presentare per i singoli e per la società[35].

26. Alù 2023.
27. Marchetti-Parona 2022.
28. Sul punto, si veda il piano *Innovate in America*. Con diverse prospettive, fra gli altri, Burt 2021; Aaronson 2020.
29. Sul punto, si veda *New Generation Artificial Intelligence Development Plan* (AIDP), su cui, fra gli altri, Roberts et al. 2021.
30. A tal proposito, Chiti-Marchetti 2020; Cath et al. 2018.
31. Art. 2, par. 1, Regolamento Ue sull'intelligenza artificiale
32. Art. 3, n. 3, Regolamento Ue sull'intelligenza artificiale.
33. Art. 3, n. 4, Regolamento Ue sull'intelligenza artificiale.
34. Mantelero 2022, p. 141.
35. AA.VV. 2023.

Secondo il modello di gestione del rischio sopra rappresentato, il Regolamento distingue i sistemi come segue:

Sistemi di IA con rischio inaccettabile: il Regolamento vieta espressamente tutte quelle pratiche il cui livello di rischio sia da ritenersi inaccettabile, in quanto contrarie ai principi ispiratori dell'ordinamento dell'Ue. Tra i trattamenti vietati dal Regolamento si annoverano[36]:

- punteggio sociale, per finalità pubbliche e private;
- sfruttamento delle vulnerabilità delle persone, utilizzo di tecniche subliminali;
- identificazione biometrica remota in tempo reale in spazi accessibili al pubblico da parte delle autorità di contrasto, fatte salve limitate eccezioni;
- categorizzazione biometrica delle persone fisiche sulla base di dati biometrici per dedurne o desumerne la razza, le opinioni politiche, l'appartenenza sindacale, le convinzioni religiose o filosofiche o l'orientamento sessuale; sarà ancora possibile filtrare set di dati basandosi su dati biometrici nel settore delle attività di contrasto;
- polizia predittiva su singoli;
- riconoscimento delle emozioni sul luogo di lavoro e negli istituti di istruzione, eccetto per motivi medici o di sicurezza (ad esempio, il monitoraggio dei livelli di stanchezza di un pilota);
- estrazione non mirata di immagini facciali da Internet o telecamere a circuito chiuso per la creazione o l'espansione di banche dati[37].

Sistemi di IA ad alto rischio: sono quelli che implicano o possono implicare un alto rischio per la salute e la sicurezza o per i diritti fondamentali delle persone fisiche, trovando così applicazione il Titolo III del Regolamento. Questi sistemi non sono di per sé vietati, ma il loro utilizzo è subordinato al rispetto di determinati requisiti obbligatori, nonché ad una duplice valutazione *ex ante*, ossia una valutazione di impatto sui diritti fondamentali ed una di conformità rispetto alla normativa applicabile[38].

La valutazione d'impatto sui diritti fondamentali (c.d. *Fundamental Rights Impact Assessment* – FRIA) – obbligo che il Regolamento pone in capo ai *deployer* – ha la finalità di valutare le categorie di persone fisiche e gruppi verosimilmente interessati dall'uso del sistema, la conformità del sistema con il diritto europeo e nazionale in materia di diritti fondamentali e l'impatto ragionevolmente prevedibile sui medesimi[39]. La valutazione di conformità (c.d. *conformity assessment*), invece – obbligo attribuito dal Regolamento ai provider – presuppone un'analisi di conformità del sistema di IA rispetto ai requisiti richiesti dall'AI Act. La procedura di valutazione dovrà essere costituita dalle seguenti fasi: (i) identificazione e analisi dei rischi noti e prevedibili associati a ciascun sistema; (ii) stima e valutazione dei rischi che possono emergere quando il sistema è usato conformemente alla sua finalità prevista e in condizioni di uso improprio ragionevolmente prevedibile; (iii) valutazione di altri eventuali rischi derivanti dall'analisi dei dati raccolti dal sistema di monitoraggio successivo all'immissione sul mercato; (iv) adozione di adeguate misure di gestione dei rischi che tengono in debita considerazione gli effetti e le possibili interazioni derivanti dall'applicazione combinata degli elementi indicati sopra alla luce dello stato dell'arte generalmente riconosciuto[40].

Ad ogni buon conto, si fa notare che siffatte operazioni di valutazione si traducono per le aziende in ingenti costi e risorse. Infatti, il bilanciamento dei diritti, così come l'analisi della compliance di un sistema di IA, rappresenta un'operazione complessa finanche per giuristi, con la conseguenza che fornitori ed utilizzatori sarebbero costretti ad esternalizzare lo svolgimento di tali valutazioni, avvalendosi di soggetti terzi qualificati. In ogni caso, anche qualora *provider* e *deployer* fossero in grado di sostenere i costi che ne deriverebbero, questi sarebbero comunque responsabili di decisioni sensibili. Non è, dunque, possibile eseguire

36. Art. 5, par. 1, Regolamento Ue sull'intelligenza artificiale.
37. Commissione europea 2023.
38. Art. 6, par. 1, Regolamento Ue sull'intelligenza artificiale.
39. Art. 27, Regolamento Ue sull'intelligenza artificiale.
40. Artt. 16 e 43 Regolamento Ue sull'intelligenza artificiale.

queste valutazioni in assenza di linee guida di settore che forniscano le corrette istruzioni da seguire. La mancanza di adeguate linee guida – necessarie a fare da bussola in analisi articolate come quelle in commento – porterebbe all'insorgere di prassi auto-regolamentative ed eccessivamente discrezionali dei destinatari di tali obblighi[41]. Inoltre, il Regolamento stabilisce che i sistemi di IA ad alto rischio devono essere progettati e sviluppati in modo tale da assicurare la tracciabilità del relativo funzionamento, che dovrà essere sufficientemente trasparente da permettere agli utilizzatori di interpretarne l'output e utilizzarlo adeguatamente[42]. I medesimi sistemi dovranno, peraltro, essere progettati in modo tale da garantire un adeguato livello di accuratezza, robustezza e cybersicurezza[43]. Gli stessi – secondo il Regolamento – dovranno essere sviluppati con strumenti di interfaccia uomo-macchina in grado di assicurare una valida supervisione da parte delle persone fisiche diretta a prevenire e contrastare i rischi per la salute, la sicurezza o i diritti fondamentali[44]. Di solito, i sistemi di IA ad alto rischio vengono utilizzati nell'ambito di dispositivi medici, veicoli, processi di recruiting, infrastrutture critiche, accesso a servizi pubblici o privati essenziali.

Sistemi di IA a rischio basso o minimo: vengono individuati per differenza rispetto ai sistemi a rischio inaccettabile o alto. Nello specifico, i sistemi di IA che comportano un rischio basso o minimo sono tutti quei sistemi leciti, chiamati esclusivamente a rispettare alcuni minimi requisiti di trasparenza. In particolare, il Regolamento richiede che il fornitore si preoccupi che la persona esposta ad un sistema di IA sia informata, in modo puntuale, chiaro e comprensibile, di stare interagendo con un sistema di IA. Inoltre, "qualora necessario", devono essere indicate quali funzioni il sistema esercita, se esiste un controllo sul sistema stesso da parte di una persona fisica, l'identificativo del responsabile del sistema, l'indicazione dei diritti della persona esposta e le azioni che la persona esposta può adottare per opporsi all'uso del sistema di IA[45]. In aggiunta ai doveri dei fornitori, il Regolamento prescrive specifici obblighi anche in capo agli utilizzatori di sistemi di IA ad alto rischio[46]. Gli utilizzatori sono, infatti, tenuti ad assicurare la correttezza e la qualità dei dati utilizzati dal sistema. Inoltre, gli utilizzatori devono rispettare le istruzioni del fornitore ma, laddove ritengano che l'uso in conformità alle istruzioni presenti un rischio, dovranno comunicarlo al fornitore stesso e, nel caso in cui quest'ultimo sia irreperibile, l'utilizzatore dovrà notificare l'incidente o il malfunzionamento alla competente autorità di controllo.

Sistemi di AI con specifici rischi di trasparenza: sistemi in relazione ai quali gli operatori devono adempiere ad obblighi sostanzialmente meno onerosi, prevalentemente di natura informativa (ad esempio, in relazione all'uso di chatbot, chiarendo agli utenti che stanno conversando con una macchina).

Con specifico riferimento ai sistemi di IA ad alto rischio, il Regolamento stabilisce, inoltre, che i fornitori debbano garantire la conformità dei propri sistemi di intelligenza artificiale ai requisiti fissati dalla normativa in esame[47]. Inoltre, una volta classificati i propri sistemi di IA come ad alto rischio, i *provider* saranno chiamati a registrare tali sistemi nella banca dati istituita a livello europeo e gestita dalla Commissione europea, di cui si dirà meglio nel prosieguo[48].

Nell'ipotesi in cui il fornitore ritenga che il proprio sistema non determini un rischio significativo tale da classificare il sistema stesso come ad alto rischio, dovrà documentare dettagliatamente la propria valutazione prima di immettere sul mercato il relativo sistema e rendere disponibile tale documentazione su richiesta dell'autorità

41. Novelli 2024, p. 100 ss.
42. Art. 13, Regolamento Ue sull'intelligenza artificiale.
43. Art. 15, Regolamento Ue sull'intelligenza artificiale.
44. Art. 14, par. 1, Regolamento Ue sull'intelligenza artificiale.
45. Considerando 72 nonché art. 13 Regolamento Ue sull'intelligenza artificiale.
46. Art. 26, Regolamento Ue sull'intelligenza artificiale.
47. Art. 8, Regolamento Ue sull'intelligenza artificiale.
48. Art. 49, Regolamento Ue sull'intelligenza artificiale.

di controllo competente a livello nazionale[49]. A seguito dell'immissione in commercio dei propri prodotti, i fornitori dei sistemi di IA ad alto rischio saranno chiamati a predisporre un programma di monitoraggio post-vendita proporzionato ai rischi del sistema immesso[50]. In tal senso, sarà allora necessaria un'analisi dei dati sulle prestazioni del sistema per l'intera durata di utilizzo del prodotto, in modo da verificarne la continua conformità con il Regolamento. Nei successivi dieci anni dall'immissione del prodotto, i provider dovranno anche conservare la documentazione tecnica, quella relativa al sistema di *quality management* e quella riguardante eventuali cambiamenti approvati dalle autorità competenti[51]. Infine, qualora un fornitore di sistemi di IA ad alto rischio ritenga che il proprio sistema, già immesso sul mercato, non sia più in linea con i requisiti previsti dal Regolamento, dovrà senza ingiustificato ritardo ritirarlo dal mercato o renderlo conforme alla normativa, nonché informare i relativi distributori e le autorità competenti. Allo stesso modo, quando un fornitore venga a conoscenza dell'esistenza di un rischio nel proprio sistema, sarà tenuto ad informare immediatamente l'autorità nazionale competente, specificando la causa della non ottemperanza e le relative azioni correttive avviate[52].

D'altro canto, anche gli utilizzatori dei sistemi ad alto rischio sono depositari di specifici obblighi da osservare. Essi sono, infatti, tenuti ad osservare le istruzioni per l'uso predisposte dal fornitore del sistema di IA, oltre che ad assicurare la correttezza dei dati di input tramite cui alimentare il sistema di intelligenza artificiale, monitorare il funzionamento del sistema di IA e segnalare eventuali rischi ed incidenti al fornitore stesso. Inoltre, gli utilizzatori sono chiamati a conservare i log dei sistemi di cui si avvalgono. Il Regolamento statuisce che – ove non diversamente previsto – tali log debbano essere conservati per un periodo di tempo non inferiore a sei mesi, precisando che, in ogni caso, dovranno essere tenuti per un tempo adeguato rispetto alla finalità del sistema e degli obblighi giuridici applicabili. Infine, gli utilizzatori di sistemi di IA ad alto rischio dovranno eseguire una valutazione d'impatto sul trattamento dei dati personali (c.d. DPIA ovvero *Data Protection Impact Assessment*) ai sensi dell'art. 35 del GDPR, avvalendosi delle informazioni che i fornitori hanno l'obbligo giuridico di rendere disponibili agli utilizzatori stessi[53].

2. Il delicato rapporto tra il Regolamento europeo sull'intelligenza artificiale e il GDPR

Il Regolamento sull'IA non è, come accennato, un atto legislativo *stand-alone*, ma si inserisce nell'ambito di una cornice normativa europea complessa e frastagliata, dove, al fine di garantire la certezza del diritto, è chiamato a coordinarsi con altre discipline proposte dalla Commissione in materia di dati e trasformazione digitale[54]. Sotto questo profilo, il grado di complessità aumenta se si considera che l'applicazione del Regolamento dovrà trovare un adeguato coordinamento anche rispetto al GDPR, data la stretta interrelazione *ratione materiae*. È chiaro, infatti, che i sistemi di intelligenza artificiale, per raggiungere un elevato grado di rendimento, necessitano di una grande mole di dati, e più è ampia la quantità di dati posta a disposizione di questi sistemi, tanto più precise sono le previsioni elaborate dagli stessi[55]. Conseguentemente, la fase più delicata per il corretto funzionamento di un sistema di intelligenza artificiale è proprio quella di raccolta dei dati[56].

Al riguardo, il Regolamento sull'intelligenza artificiale non si occupa della raccolta e del trattamento dei dati, i quali rimangono pertanto regolati dalla normativa vigente e, in particolare, dal GDPR. Trascorso, dunque, il momento di raccolta dei dati, è fondamentale comprendere quale sia la

49. Art. 16, Regolamento Ue sull'intelligenza artificiale.
50. Art. 72, Regolamento Ue sull'intelligenza artificiale.
51. Artt. 16 e 18, Regolamento Ue sull'intelligenza artificiale.
52. Art. 20, Regolamento Ue sull'intelligenza artificiale.
53. Art. 26, Regolamento Ue sull'intelligenza artificiale.
54. Iacovelli-Fontana 2022, pp. 117-119.
55. Finocchiaro 2019.
56. Si veda, al riguardo, Colapietro-Moretti 2020, pp. 376-377.

normativa applicabile, una volta che tali dati vengano immessi nel sistema.

Considerati gli ampi margini di potenziale sovrapposizione, l'attuazione delle due discipline potrebbe portare ad un eccesso di regolamentazione. Per questo motivo, il rapporto simbiotico tra protezione dei dati personali e intelligenza artificiale deve porsi al centro dell'esame e della relativa attuazione dell'AI Act, al fine di prevenire eventuali contrasti o contrapposizioni con la disciplina complementare del GDPR[57]. Con specifico riguardo a questo punto, la stessa Commissione europea, nella propria relazione esplicativa di accompagnamento del Regolamento sull'IA, chiarisce che quest'ultimo non pregiudica l'applicabilità del GDPR. È una considerazione in qualche modo ovvia, dal momento che il GDPR è finalizzato a proteggere un diritto fondamentale, già previsto dagli articoli 8 della Carta dei diritti fondamentali dell'Unione europea e 16 TFUE[58]. Da una tale constatazione deriva che non sarebbe possibile risolvere eventuali conflitti tra fonti normative invocando il principio di specialità. Invero, non avrebbe senso sostenere la prevalenza del Regolamento sull'intelligenza artificiale rispetto al GDPR sulla base di un principio di specialità, considerato che la seconda normativa è volta ad attuare un diritto umano fondamentale espressamente previsto da una fonte primaria. Si può, dunque, affermare che entrambe le fonti in esame dovranno essere applicate ed implementate cumulativamente tra loro[59].

Inevitabilmente, dunque, il Regolamento sull'IA e il GDPR presentano numerosi punti di contatto rispetto alle proprie modalità di regolazione. Le similitudini tra le due fonti normative si riscontrano già nello strumento giuridico prescelto dal legislatore europeo: in entrambi i casi, l'Unione europea ha adottato la forma del regolamento in luogo della direttiva, al fine di consolidare un quadro normativo omogeneo e prevalentemente rigido per gli Stati Membri, prevedendo sempre meccanismi di revisione periodica per assicurare discipline "*stable but not still*"[60]. La scelta della fonte utilizzata, come è evidente, costituisce un fil rouge che collega tutti gli atti normativi della politica europea sul digitale, in linea con la volontà di inaugurare una governance dell'innovazione incentrata sul principio del "*one continent, one law*"[61].

Altra analogia tra i due testi normativi è, certamente, la scelta della medesima cornice strutturale che fa da sfondo alle relative discipline, ossia il c.d. *risk based approach* (fondato su di una piramide di gravità ascendente), dove sono le stesse organizzazioni a dover dimostrare la propria conformità al dettato legislativo. In tal senso, come già evidenziato, l'AI Act classifica i sistemi di intelligenza artificiale in base al rischio generato per gli utilizzatori, fissando specifici obblighi per fornitori ed utilizzatori di entità crescente in base al livello di rischio considerato. In particolare, in analogia con gli artt. 25 e 35 del GDPR, l'AI Act impone ai *provider* di implementare un sistema di gestione del rischio atto a mappare i rischi conosciuti e quelli prevedibili e a mitigarli, di informare gli interessati della loro esistenza, nonché di monitorare ed aggiornare in via periodica il sistema di *risk assessment*. La valorizzazione dell'autonoma valutazione dell'operatore risponde ad una logica di responsabilizzazione e *accountability* già centrale nell'impianto giuridico del GDPR[62].

Ciononostante, i punti di contatto con il GDPR non si esauriscono nell'approccio basato sul rischio: infatti, il Regolamento richiama anche principi e meccanismi tipici del sistema di governance e di gestione dei dati del GDPR, impiegandoli come strumenti per un corretto e trasparente addestramento dei sistemi di IA[63]. Tra questi, si riportano di seguito i principali elementi in comune.

Extraterritorialità: l'AI Act persegue anche obiettivi di natura geopolitica, cercando di estendere l'ambito di applicazione del Regolamento. L'art. 2, infatti, con tecnica analoga a quella utilizzata

57. Cerrina Feroni 2023.
58. Si veda, a tal proposito, Pollicino-Bassini 2017, pp. 135-136; Calzolaio 2017, p. 594.
59. Contaldi 2021, p. 1199 ss.
60. Casonato-Marchetti 2021, pp. 419-421.
61. Commissione Europea 2015.
62. Mantelero-Poletti 2018, p. 73.
63. AssoDPO 2023.

dall'art. 3 del GDPR, dispone che il Regolamento si applichi ai fornitori che immettono sul mercato o mettono in servizio sistemi di intelligenza artificiale nell'Unione, indipendentemente dal fatto che siano stabiliti nell'Unione o in un Paese terzo, nonché agli utilizzatori dei sistemi di IA situati nell'Unione e ai fornitori e agli utilizzatori di sistemi di IA situati in un Paese terzo, ove l'output prodotto dal sistema sia utilizzato nell'Unione.

Qualità ed esattezza dei dati: quello della qualità e dell'accuratezza dei dati è uno dei requisiti per la messa in commercio dei sistemi di IA ad alto rischio. È una specificità introdotta dall'art. 10 del Regolamento, che prevede al comma 3 che i set di dati utilizzati per l'addestramento dei modelli debbano essere «sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista»[64]. Nonostante ogni principio debba essere letto nello specifico contesto dove è inserito, è immediato il parallelismo con i principi applicabili al trattamento dei dati personali elencati all'art. 5 GDPR, dove si trovano, tra gli altri, il principio di minimizzazione, di esattezza, di integrità.

Privacy by design e *by default*: il Regolamento statuisce che i sistemi di IA, e, nello specifico, quelli che prevedono l'uso di dati per l'addestramento di modelli, debbano essere sviluppati considerando una molteplicità di elementi, tra cui: la raccolta di dati; le operazioni di trattamenti pertinenti ai fini della preparazione dei dati, compresi la pulizia dei dati, l'aggregazione, l'arricchimento; una valutazione preliminare della disponibilità, della quantità e dell'adeguatezza dei set di dati necessari; l'individuazione di eventuali lacune o carenze nei dati e il modo con cui possono essere colmate. Il metodo prescelto dal Regolamento pare, quindi, ispirarsi ai principi di *privacy by design* e *by default* di cui all'art. 25 GDPR, che richiedono che ogni progetto avente ad oggetto dati personali sia pensato fin dalla sua ideazione secondo un'impostazione *privacy friendly*, ovvero minimizzando e calibrando i dati personali trattati strettamente necessari per il raggiungimento delle finalità del progetto stesso.

Principio di trasparenza: il Regolamento fissa specifici doveri di trasparenza, nella misura in cui prevede che i sistemi di intelligenza artificiale ad alto rischio debbano essere progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli utilizzatori di interpretare l'output del sistema e utilizzarlo adeguatamente. Anche tale previsione sembra richiamare uno dei principi portanti del GDPR e, in particolare, il principio di trasparenza formalizzato dall'art. 5 del GDPR che mette in capo ai titolari del trattamento l'obbligo di rendere gli interessati consapevoli di come verranno trattati e successivamente conservati i dati personali in relazione allo specifico trattamento svolto, nonché dei rischi ad esso correlati. Quest'obbligo di trasparenza si concretizza nel rispetto dei doveri informativi di cui gli artt. 13 e 14 del GDPR che prevedono che il titolare – prima di avviare un trattamento di dati personali – fornisca ai relativi soggetti interessati un'idonea informativa privacy, tramite cui esporre le modalità con cui saranno trattati i dati personali raccolti.

Processi decisionali automatizzati: l'art. 22 del GDPR, che disciplina il trattamento di dati personali che avviene per mezzo di processi decisionali automatizzati, costituisce il maggior punto di contatto con l'AI Act, dal momento che tale disposizione normativa ha ad oggetto proprio fattispecie di trattamento, come la profilazione, effettuate con il ricorso all'intelligenza artificiale. Invero, giova notare come, mentre la logica perseguita dall'AI Act presuppone di *default* lo svolgimento di processi decisionali automatizzati – seppure controllati attraverso un'attenta sorveglianza umana – l'art. 22 del GDPR, *a contrario*, sancisce il diritto per gli interessati di non essere sottoposti ad una decisione basata unicamente sul trattamento automatizzato finalizzata all'assunzione di una decisione rilevante per la propria sfera giuridica. Ciononostante, l'art. 22 non fissa un divieto assoluto ma, tramite una clausola di apertura *ad hoc*, ammette un trattamento automatizzato di dati personali quando questo sia necessario all'esecuzione di un contratto di cui è parte l'interessato, quando sia autorizzato dal diritto dell'Unione, oppure quando vi sia il consenso dell'interessato stesso[65]. A tal proposito, è interessante notare come – nonostante sia il GDPR a prevedere un divieto relativo rispetto a trattamenti automatizzati di dati personali

64. Art. 10, par. 3, Regolamento Ue sull'intelligenza artificiale.

65. Per una disamina approfondita in materia si veda Napoli 2020, pp. 326-329.

che, tuttavia, non esclude aprioristicamente ma consente alle condizioni sopra menzionate – è però l'AI Act a vietare espressamente alcuni processi decisionali automatizzati (tra cui, a titolo esemplificativo, il *social scoring*) che, ai sensi della normativa privacy, sarebbero stati ammessi seppur con adeguate cautele e misure. In tal senso, è bene allora riflettere sulle ricadute che le incongruenze sopra delineate tra le due fonti normative potrebbero avere sul piano pratico, specialmente se si pensa ai contesti di lavoro aziendali, dove spesso esigenze di business portano a considerare progetti complessi e talvolta basati sull'uso dell'intelligenza artificiale.

Tirando le fila di quanto sopra analizzato, è possibile affermare che, nonostante le molteplici similitudini riscontrabili tra GDPR ed AI Act, resta essenziale focalizzarsi sull'assenza, allo stato attuale, di un meccanismo di raccordo procedurale adeguato tra le due discipline, che determina l'insorgere di almeno tre profili di criticità[66].

In primo luogo, si corre il rischio di imporre obblighi eccessivi agli attori privati, che dovranno quindi rileggere l'applicazione dell'art. 22 del GDPR alla luce del ben più ampio panorama dell'intelligenza artificiale.

In secondo luogo, senza idonee linee guida delle competenti autorità di controllo, gli operatori di mercato – sovente provenienti da sistemi giuridici diversi da quello europeo dove la protezione dei dati non è analogamente forte – saranno costretti ad espletare personalmente un bilanciamento tra gli interessi in gioco, giungendo a valutazioni arbitrarie e discrezionali. In tale contesto, forme di *self-regulation*[67], laddove esistenti, dovrebbero svolgere una mera funzione integrativa o complementare rispetto alla regolazione primaria[68], senza assorbire completamente i contenuti regolativi di quest'ultima, poiché diversamente s'incorrerebbe nel rischio che i pubblici poteri abdichino del tutto al compito essenziale di operare bilanciamenti tra valori, interessi e posizioni soggettive diverse[69].

In terzo luogo, la somma delle considerazioni precedenti, in aggiunta all'incertezza normativa, sortirebbe l'effetto di diminuire il raggio di tutela del singolo individuo[70]. Al riguardo, il fenomeno dell'*over-regulation*[71] è sempre un'arma a doppio taglio, nella misura in cui, se è vero che garantisce l'esistenza di più normative che da fronti diversi proteggono gli stessi diritti, dall'altro, se non ben regolato, rischia di ottenere l'effetto opposto alla finalità iniziale, mettendo a rischio quegli stessi diritti che si prefiggeva di tutelare.

3. Il sistema sanzionatorio dell'AI Act: luci ed ombre

Un altro profilo di necessaria comparazione tra le due normative in oggetto è rappresentato dal sistema sanzionatorio. A tal riguardo, si evidenzia che il Regolamento inaugura un sistema sanzionatorio fondato sul principio di diretta proporzionalità e modellato, dunque, in relazione alla gravità della violazione, nonché delle dimensioni e del fatturato dell'operatore che ha commesso la sanzione. Non a caso, infatti, le misure sanzionatorie introdotte dall'AI Act variano sia per intensità sia per tipologia della sanzione in ragione di una molteplicità di criteri di riferimento.

Più dettagliatamente, il Regolamento prevede sanzioni che – in linea con quanto già previsto nel GDPR – sono parametrate al fatturato annuo globale riferito all'esercizio finanziario precedente del soggetto giuridico cui la violazione è contestata. Nello specifico, sono previste sanzioni fino: (i) al 7% del fatturato o a 35 milioni di euro per la violazione delle norme in materia di pratiche vietate o di non conformità ai requisiti relativi alla qualità dei dati; (ii) al 3% o a 15 milioni di euro per la gran parte delle altre violazioni, ivi incluse quelle relative alle disposizioni in materia di *General-purpose AI models*; (iii) all' 1,5% del fatturato o a 7,5 milioni

66. Sul punto, si veda, *inter alia*, Faini 2020, pp. 90-91.
67. Parona 2020.
68. Concordemente, si veda De Minico 2020, pp. 16-17.
69. Stradella 2019, p. 8.
70. De Gregorio-Paolucci 2022.
71. Si veda al riguardo Raffiotta 2023.

di Euro per la violazione di obblighi informativi[72]. Spetterà, poi, ai singoli Stati Membri implementare e articolare la disciplina sanzionatoria di dettaglio a livello nazionale. A valle dell'ormai vicina approvazione formale del testo, l'AI Act sarà produttivo di effetti giuridici secondo tempistiche differenti. In particolare, le disposizioni aventi ad oggetto le sanzioni saranno pienamente in vigore dodici mesi dopo l'approvazione del Regolamento. Conseguentemente, nei prossimi mesi, sarà di primaria importanza per *deployer* ed utilizzatori di sistemi di intelligenza artificiale attuare i necessari presidi contrattuali e di *compliance* richiesti dal Regolamento in commento.

L'apparato sanzionatorio introdotto dal Regolamento rievoca, per natura e caratteristiche costitutive, quello posto in essere dal GDPR. Invero, quest'ultimo stabilisce un impianto sanzionatorio che, come l'AI Act, impattando fortemente sul fatturato dei soggetti coinvolti, comprende sanzioni amministrative pecuniarie diverse a seconda del tipo di violazione accertata e della previsione normativa violata. Più nello specifico, gli articoli 83 e 84 del GDPR regolano rispettivamente le condizioni generali per infliggere sanzioni amministrative pecuniarie e l'entità di tali sanzioni. Queste ultime raggiungono un importo fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per le violazioni meno gravi; mentre, per le infrazioni più gravi, si giunge fino ad un ammontare pari a 20 milioni di euro o fino al 4% del fatturato mondiale annuo precedente, se superiore, per le imprese. Inoltre, anche l'AI Act, come il GDPR, attribuisce all'autorità di controllo competente il compito di infliggere e determinare l'ammontare delle sanzioni, valutando caso per caso l'*an* e il *quantum* in base alle circostanze concrete, tra cui l'entità della violazione, la sua durata e il dolo o la colpa dell'autore. Ancora una volta, con l'AI Act, il legislatore europeo, così come già fatto con il GDPR, lascia all'organo di controllo un ampio margine di discrezionalità entro cui muoversi per esercitare il proprio potere sanzionatorio. Se ne trae la considerazione che, giacché spesso l'uso di un sistema di intelligenza artificiale presuppone ed implica un trattamento di dati personali, sarà difficile per la futura autorità di controllo far coesistere e coordinare tra loro il regime sanzionatorio dell'AI Act con quello del GDPR. Tale situazione di incertezza normativa è ancora più chiara se si tiene in debita considerazione l'assenza di apposite previsioni atte a regolare il rapporto tra le due discipline sanzionatorie e la probabilità che possa essere individuata come autorità di controllo competente per la regolazione dell'intelligenza artificiale un organo diverso dall'Autorità Garante per la protezione dei dati personali.

Nonostante la rilevanza delle misure sanzionatorie e la possibilità per le autorità di richiedere il ritiro dal mercato o il richiamo dei prodotti, la disciplina complessiva non appare del tutto sufficiente a garantire un'applicazione efficace. L'esperienza del GDPR mostra che un eccessivo affidamento sull'*enforcement* delle autorità nazionali si espone al rischio di difformità applicative, a causa delle notevoli divergenze di risorse e prassi di intervento nei diversi Stati membri. Com'è usuale in campo tecnologico, poi, si pone il problema di possibili difformità nei criteri di valutazione degli standard tecnici, che sarà tanto più pregnante in un settore, quello dell'IA, caratterizzato da un elevato numero di attori e di standard diversi. Infine, occorre segnalare che il Regolamento non contiene meccanismi di azione per gli individui o gruppi danneggiati, nemmeno nella forma di reclamo. L'assenza di tali previsioni, che avrebbero compensato i limiti dell'*enforcement* pubblico, risulta certamente criticabile, avendo come effetto anche il ridimensionamento del ruolo della società civile nello sviluppo affidabile dell'IA[73].

4. Il sistema di governance dell'AI Act: la delicata scelta di un'autorità di controllo nazionale per regolare l'intelligenza artificiale

Il Regolamento delinea un sistema di governance che è possibile definire congiuntamente come "multilivello" e "multistakeholder"[74]. Ciò in quanto i meccanismi di governance messi a punto dal Regolamento agiscono sia a livello europeo sia a

72. Art. 99, Regolamento Ue sull'intelligenza artificiale.

73. Contissa et al. 2021, pp. 31-33.

74. Sul tema della governance, cfr. Pajno et al. 2019, p. 219.

livello nazionale per singolo Stato Membro, coinvolgendo inoltre una pluralità di attori.

Con riferimento al livello Ue, il Regolamento istituisce il Comitato europeo per l'Intelligenza artificiale (*European Artificial Intelligence Board*), la cui composizione riflette la logica di cooperazione istituzionale tra autorità di controllo nazionali e autorità di riferimento Ue che caratterizza la maggior parte degli atti normativi europei[75]. Infatti, il Comitato sarà composto da un rappresentante dell'autorità di vigilanza nazionale per Stato Membro e dal Garante europeo per la protezione dei dati (*European Data Protection Supervisor* – EDPS), mentre la presidenza sarà affidata alla Commissione. Per quanto concerne i poteri del Comitato, il Regolamento prevede che il Board dovrà principalmente garantire la cooperazione tra le autorità nazionali e supportare l'attività della Commissione tramite l'emanazione di pareri, raccomandazioni e linee guida, con un ruolo, quindi, eminentemente consultivo[76]. Pur limitandosi all'emanazione di atti di *soft law*, il supporto del Board sarà, tuttavia, essenziale per garantire un corretto e adeguato svolgimento dei compiti attribuiti in questa delicata materia alla Commissione europea, tra cui giova ricordare anche la complessa attività di tenuta e controllo della sopra accennata banca dati europea sui sistemi di intelligenza artificiale ad alto rischio[77]. Tale banca dati – che sarà creata e gestita dalla Commissione in collaborazione con gli Stati Membri – conterrà tutte le informazioni relative ai sistemi di IA ad alto rischio destinati al mercato europeo che i *provider* saranno tenuti a comunicare, ed avrà la finalità di assicurare un regime di controllabilità e pubblicità della circolazione di tali prodotti all'interno dell'Ue[78].

All'interno della stessa Commissione, il Regolamento sancisce, inoltre, l'istituzione di un *AI Office*, che supervisionerà l'applicazione e il rispetto delle disposizioni dell'AI Act[79]. Accanto ad essi, saranno poi costituiti (i) un *Advisory Forum* composto da stakeholder rappresentativi di industria, società civile e accademia, con funzioni consultive[80] e (ii) un *Scientific Panel of independent experts*, che avrà il compito di supportare l'AI Office nell'attività di corretta attuazione delle previsioni del Regolamento, con particolare riferimento ai *General-purpose AI models*[81].

Spostando l'attenzione sul livello nazionale di governance, invece, gli Stati Membri saranno chiamati ad individuare almeno: (i) un'autorità "di notifica" responsabile di istituire e attuare le procedure necessarie per la valutazione e notifica degli organismi di valutazione della conformità dei sistemi ad alto rischio e per il loro monitoraggio; (ii) un'autorità di sorveglianza del mercato, con poteri investigativi e correttivi, tra cui anche quello di accedere ai dati personali in fase di elaborazione e alle informazioni necessarie per eseguire i loro compiti[82].

In Europa, il primo tentativo di dare attuazione alle previsioni in materia di governance dell'AI Act si è ha avuto di recente in Spagna, dove nel settembre 2023 è stata istituita l'*Agencia Española de Supervisión de Inteligencia Artificial* ("AESIA"), ovvero la prima autorità di controllo in materia di intelligenza artificiale in Europa[83]. Prevista come parte integrante della Strategia nazionale spagnola per l'intelligenza artificiale, l'istituzione dell'AESIA si pone in netto anticipo rispetto all'entrata in vigore dell'AI Act, collocando la Spagna in posizione di avanguardia nel panorama europeo. La natura dell'Agenzia riflette la scelta della Spagna di costituire una nuova autorità di vigilanza anziché assegnare tale ruolo ad un organo già esistente, alimentando così gli orientamenti e le attenzioni del dibattito dottrinale attualmente in corso sul tema. Secondo quanto si evince dalla lettura dello

75. Carantani 2024.
76. Artt. 65 e 66, Regolamento Ue sull'intelligenza artificiale.
77. Art. 71, Regolamento Ue sull'intelligenza artificiale.
78. Casonato-Marchetti 2021, pp. 434-435.
79. Art. 64, Regolamento Ue sull'intelligenza artificiale.
80. Art. 67, Regolamento Ue sull'intelligenza artificiale.
81. Art. 68, Regolamento Ue sull'intelligenza artificiale.
82. Capacci-Galli-Loreggia-Maroccia 2024, pp. 8-9.
83. Al riguardo, si veda Valdés Borruey-Latasa Vassallo-Ñíguez Olalla 2023.

Statuto dell'Agenzia – pubblicato sul *Boletín Oficial del Estado* all'interno del Real Decreto 729/2023 del 22 agosto – l'AESIA sarà responsabile dell'intera materia dell'intelligenza artificiale e, in particolare, della corretta implementazione del Regolamento europeo sull'IA. L'Agenzia avrà prevalentemente compiti di supervisione, consulenza, sensibilizzazione, formazione e finanche poteri ispettivi e sanzionatori. Quanto alla natura giuridica, l'Agenzia farà capo al Ministero degli Affari economici e della Trasformazione digitale, attraverso il Segretario di Stato sulla Digitalizzazione e Intelligenza Artificiale cui spetterà il ruolo di Presidente, e godrà di personalità giuridica pubblica, con patrimonio proprio e autonomia di gestione. In linea con quanto enunciato dal suo Statuto, l'AESIA eserciterà le proprie attività ispirandosi ai principi di interesse generale, autonomia, indipendenza tecnica e trasparenza, efficacia ed efficienza, cooperazione interistituzionale ed uguaglianza[84].

In Italia, la scelta in merito all'individuazione dell'autorità di controllo competente sembrerebbe ancora aperta. In tale contesto, infatti, è al momento in corso un vivace dibattito politico-istituzionale che vede su due posizioni differenti, da un lato, il Governo e, dall'altro, l'Autorità Garante per la protezione dei dati personali. In particolare, dal fronte dell'esecutivo, è stato approvato dal Consiglio dei Ministri del 23 aprile 2024 un disegno di legge «per l'introduzione di disposizioni e la delega al Governo in materia di intelligenza artificiale» che attribuisce le funzioni di supervisione e controllo richieste dall'AI Act all'Agenzia per l'Italia Digitale ("AgID") e quelle relative alla cybersecurity all'Agenzia per la cybersicurezza nazionale ("ACN"). La scelta di affidare ad AgID ed ACN – agenzie entrambe soggette alle funzioni di indirizzo e coordinamento della Presidenza del Consiglio – il potere di vigilanza in materia di intelligenza artificiale intende rispecchiare la vision strategica del Governo italiano incentrata sull'efficacia e l'efficienza nella governance dell'IA. Tali agenzie sono, in effetti, dotate di competenze complementari e altamente specializzate da considerarsi essenziali per affrontare le sfide poste dall'intelligenza artificiale in ambito di cittadinanza, industria, sicurezza, protezione dei dati e sicurezza nazionale. Di contro – ad avviso del Governo – la scelta di attribuire questo ruolo ad un'autorità amministrativa indipendente porterebbe con sé alcune difficoltà applicative, dal momento che le Authority potrebbero non avere quelle competenze tecniche e digitali, oltre che l'integrazione con il sistema digitale nazionale, già in possesso di AgID e ACN[85].

Dal canto suo, l'Autorità Garante per la protezione dei dati personali si è più volte espressa in ordine al sistema di governance delineato dall'AI Act[86], sottolineando l'importanza di individuare un'autorità autonoma e neutrale. In una segnalazione inviata ai Presidenti di Senato e Camera e al Presidente del Consiglio[87], l'Autorità ha ricordato che il Regolamento si fonda sull'articolo 16 del Trattato sul funzionamento dell'Unione europea – che è la base giuridica della normativa di protezione dei dati – e che lo stesso Regolamento prevede il controllo delle autorità di protezione dei dati personali su processi algoritmici che utilizzino dati personali. Conseguentemente, ha ribadito che siffatte autorità sono gli unici organi effettivamente destinatari di una riserva di competenza sancita dall'AI Act e, in quanto indipendenti, legittimate a svolgere le funzioni di controllo in settori delicati come quello delle attività di contrasto. Segnatamente, l'Autorità ha colto l'occasione per evidenziare nuovamente di essere in possesso di quei requisiti di competenza e indipendenza necessari per attuare il Regolamento con l'obiettivo di un livello elevato di tutela dei diritti fondamentali. Al riguardo, il Garante sottolinea che tale scelta avrebbe anche il merito di generare una semplificazione per gli utenti, che potrebbero così rivolgersi ad un'unica autorità per questioni inerenti a sistemi di intelligenza artificiale che trattino dati personali, senza il rischio di conflitti di competenza o di duplicazione di oneri amministrativi.

Come è evidente, l'attribuzione a livello nazionale del ruolo di autorità di controllo per l'intelligenza artificiale costituisce un *thema decidendum* assai complesso, articolato su una pluralità di posizioni e considerazioni non sempre inconciliabili.

84. Catanzano 2023.

85. Cfr. Anastasio 2024; Esperti 2024; Donatio 2024.

86. Garante per la protezione dei dati personali 2022.

87. Garante per la protezione dei dati personali 2024.

Ciò che emerge da un'analisi macroscopica della questione è la stringente necessità di dar vita ad una concreta alleanza di sistema tra soggetti con un ruolo neutro e di garanzia ma anche provvisti di consolidate strutture tecniche, nel solco, ovviamente, di un quadro normativo interno chiaro, sia in merito al riparto di competenze, sia in relazione agli ambiti di collaborazione. Solo attraverso un modello di intenso coordinamento tra competenze, sensibilità e strutture si potrà rimanere in linea con l'obiettivo di fondo della disciplina europea, ossia assicurare il funzionamento di strumenti di tutela giuridicamente effettivi, a tutela delle libertà degli utenti e in grado di promuovere il pieno sviluppo del mercato unico digitale.

5. Conclusioni

Come tutti gli strumenti normativi che si prefiggono l'obiettivo di essere *maxima summa* di un panorama complesso e frastagliato, così come quello delineato dall'intelligenza artificiale, anche l'AI Act non può essere esente da riflessioni e prospettive *de iure condendo*, strumentali ad una migliore interiorizzazione dei suoi contenuti.

In primo luogo, va evidenziato come l'impianto normativo in questione appaia inevitabilmente rigido. Invero, l'intenzione del legislatore europeo di mappare ogni possibile tipologia di sistema di intelligenza artificiale, categorizzata per livello di rischio, pur essendo lodevole dal punto di vista formale, in quanto volta a garantire esaustività dei contenuti e completezza della normazione, corre, tuttavia, il rischio di risultare nel breve periodo anacronistica e desueta. È un fatto che l'evoluzione della tecnica nel campo dei sistemi di intelligenza artificiale proceda incessantemente e a grande velocità: ciò comporta che, facilmente, le previsioni del Regolamento potrebbero non essere in linea con le tecnologie nel frattempo subentrate[88], per quanto la stessa classificazione dei sistemi di IA sarà soggetta a revisione periodica, come previsto dal Regolamento stesso. Quest'ultimo, come il GDPR, introduce un sistema giuridico fondato sulla gestione del rischio ma, a differenza del regolamento sulla protezione dei dati, non contempla l'applicazione del principio di *accountability*, in forza del quale il titolare del trattamento è tenuto ad applicare le disposizioni regolamentari in conformità alle caratteristiche proprie del trattamento di dati personali e dimostrare di aver adeguatamente attuato la *compliance* richiesta. Tale responsabilizzazione imposta dal GDPR al titolare del trattamento consente un costante adattamento del modello di gestione del rischio in grado di rendere sempre flessibile il dettato normativo. Al contrario, nell'AI Act questa tendenza si inverte ed è, quindi, lo stesso legislatore europeo che ha l'onere di individuare quali sistemi di intelligenza artificiale siano da considerare ad alto rischio e come tali rischi debbano essere mitigati. Conseguentemente, la staticità dell'approccio introdotto dal Regolamento pone come criticità quella di avere un sistema non abbastanza dinamico rispetto ai continui sviluppi dell'intelligenza artificiale.

In secondo luogo, va evidenziato che il Regolamento presenta un meccanismo di tutela dei diritti e delle libertà della persona molto più ristretto e contenuto rispetto a quello offerto dal GDPR. Infatti, mentre nel GDPR gli interessati hanno un'ampia gamma di diritti da poter esercitare nei confronti dei titolari del trattamento dei dati, in aggiunta agli strumenti delle segnalazioni e dei reclami da esercitare direttamente dinanzi alle autorità di controllo, nell'AI Act i rimedi riconosciuti agli interessati sono soltanto due. Da un lato, vi è la possibilità di presentare un reclamo dinanzi all'autorità di sorveglianza del mercato per violazioni del Regolamento e, dall'altro, è possibile esercitare, nei confronti del produttore di sistemi di IA ad alto rischio, il diritto a ricevere spiegazioni circa eventuali decisioni assunte sulla base dei risultati del sistema che incidano sui diritti e le libertà del soggetto istante. La mancanza di centralità dei diritti degli interessati e l'assenza di un regime di liability chiaro all'interno dell'AI Act lascia presumere, quindi, che – almeno per affinità di materia – il sistema di presidi sarà integrato dalle disposizioni su diritti, segnalazioni e reclami già previsti in materia di protezione dei dati personali.

Ulteriori criticità sorgono anche in relazione ai rinvii effettuati dal Regolamento al GDPR. In questo senso, infatti, nei punti in cui l'AI Act rinvia al GDPR sarebbe utile determinare in modo più chiaro i rapporti tra le due fonti regolatorie, assicurando un miglior coordinamento tra le diverse discipline. D'altro canto, nei casi in cui il

88. Cfr. Finocchiaro 2012.

Regolamento non rinvii espressamente al GDPR, si potrebbe essere indotti a pensare che sia ammissibile una deroga alla normativa sul trattamento dei dati personali[89].

In ultima analisi, va sottolineato come l'AI Act sia solo l'ultimo dei numerosi interventi normativi di questa legislatura europea sul mercato unico digitale.

Nella non facile opera di coordinamento[90] cui sarà chiamato il rinnovato legislatore europeo, sarebbero auspicabili alcune modifiche contestuali non solo al testo dell'AI Act ma anche a quello del GDPR, volte a migliorare il coordinamento e l'interrelazione tra le due discipline, in un'ottica di complessiva semplificazione del sistema.

In questa direzione, sembra parimenti auspicabile la predisposizione di un'opera di codificazione e coordinamento della pluralità delle fonti normative applicabili al settore del digitale[91], come strumento di prevenzione del rischio patologico di ipertrofia normativa[92].

Tale lavoro di riordino della materia appare di stringente urgenza, al fine di scongiurare il rischio che il legislatore europeo ha strenuamente cercato di evitare in questi ultimi anni, ossia rallentare il processo di digitalizzazione – proprio a causa della moltitudine di vincoli normativi incombenti sugli operatori di mercato – senza nemmeno innalzare il livello di tutela dei diritti dei cittadini dell'Unione[93]. In conclusione, la sistematizzazione della fitta trama normativa ad oggi esistente in Europa potrebbe rappresentare la via maestra da percorrere per orientare – senza frenare – lo sviluppo tecnologico[94], creando un ecosistema europeo aperto all'innovazione e concretamente in grado di sconfessare l'annoso leitmotiv «America innovates, China replicates, Europe regulates»[95].

Riferimenti bibliografici

S.A. Aaronson (2020), *America's uneven approach to AI and its consequences*, Working paper 2020-7, Institute for International Economic Policy Working Paper Series, George Washington University, April 2020

AA.VV. (2023), *L'Unione Europea approva l'AI Act*, Newsletter Bonelli Erede, 20 dicembre 2023

A. Alù (2023), *I differenti approcci regolatori in materia di intelligenza artificiale tra evoluzione tecnologica e risvolti applicativi*, in "Il Diritto di famiglia e delle persone", 2023, n. 3

P. Anastasio (2024), *Intelligenza Artificiale, ora è ufficiale: la vigilanza in Italia ad AgID e ACN*, in "Key-4Biz", 20 marzo 2024

AssoDPO (2023), *AI ACT, la meta è vicina: un nuovo standard globale*, 19 dicembre 2023

J. Black, A. Murray (2019), *The Regulatory Action – Regulating AI and Machine Learning: Setting the Regulatory Agenda*, in "European Journal of Law and Technology", vol. 10, 2019, n. 3

A. Bradford (2021), *Effetto Bruxelles. Come l'Unione Europea regola il mondo*, Franco Angeli, 2021

F. Bravo (2021), *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in "Contratto e impresa Europa", 2021, n. 1

A. Burt (2021), *New AI Regulations Are Coming. Is Your Organization Ready?*, in "Harvard Business Review", April 30, 2021

89. Iacovelli-Fontana 2022, pp. 136-138.
90. In questo senso, cfr. Black-Murray 2019.
91. Contaldi 2021, p. 1213.
92. Torreggiani 2021.
93. In tal senso, Miniscalco 2020, p. 260.
94. Frosini 2022, p. 13.
95. Cfr., *inter alia*, Faralli 2019.

S. Calzolaio (2017), *Protezione dei dati personali*, in "Digesto delle Discipline Pubblicistiche. Aggiornamento VII", Utet, 2017

A. Capacci, G. Galli, A. Loreggia, I. Maroccia (2024), *Il nuovo regolamento europeo sull'IA: cosa cerca di fare e cosa fa*, in "Osservatorio sui Conti Pubblici Italiani", 22 febbraio 2024, pp. 8-9

I. Carantani (2024), *IA Act: l'Unione Europea approva la proposta di Regolamento sull'intelligenza artificiale*, in "Ius in itinere", 3 maggio 2024

C. Casonato, M. Fasan, S. Penasa (a cura di) (2022), *Diritto e Intelligenza Artificiale*, in "DPCE Online", 2022, n. 1

C. Casonato, B. Marchetti (2021), *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in "BioLaw Journal – Rivista di Bio Diritto", 2021, n. 3

L. Catanzano (2023), *Il Regno dell'Intelligenza Artificiale: la Spagna istituisce la prima agenzia statale di supervisione dell'IA in Europa*, in "Fondazione Leonardo – Civiltà delle Macchine", 11 ottobre 2023

C. Cath, S. Watcher, B. Mittelstadt, M. Taddeo, L. Floridi (2018), *Artificial intelligence and the "Good Society": the US, EU and UK approach*, in "Science and Engineering Ethics", 2018, n. 2

G. Cerrina Feroni (2023), *Intelligenza artificiale e ruolo della protezione dei dati personali*, 14 febbraio 2023

G. Cerrina Feroni (2022), *Luci e ombre della Data Strategy europea*, 13 maggio 2022

E. Chiti, B. Marchetti (2020), *Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale*, in "Rivista della Regolazione dei mercati", 2020, n. 1

C.A. Ciaralli (2023), *Intelligenza artificiale, decisione politica e transizione ambientale: sfide e prospettive per il costituzionalismo*, in "federalismi.it", 2023, n. 15

C. Colapietro, A. Moretti (2020), *L'Intelligenza Artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali*, in "BioLaw Journal – Rivista di BioDiritto", 2020, n. 3

Commissione europea (2023), *Intelligenza artificiale – Domande e risposte*, 12 dicembre 2023

Commissione Europea(2015), *Agreement on Commission's EU data protection reform will boost Digital Single Market*, December 15, 2015

G. Contaldi (2021), *Intelligenza artificiale e dati personali*, in "Ordine internazionale e diritti umani", 2021, n. 5

G. Contissa, F. Galli, F. Godano, G. Sartor (2021), *Il Regolamento europeo sull'intelligenza artificiale: analisi informatico-giuridica*, in "i-lex – Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale", 2021, n. 2

G. De Gregorio, F. Paolucci (2022), *Dati personali e AI Act*, in "Media Laws. Law and Policy of the Media in a Comparative Perspective", April 15, 2022

G. De Minico (2023), *Relazione introduttiva*, in G. De Minico, M. Villone (a cura di), "Stato di diritto – Emergenza – Tecnologia", Consulta on line, 2020

I. Donatio (2024), *IA, Butti: presto Ddl, prevista Agenzia e non Autorità indipendente*, in "The Watcher Post", 12 marzo 2024

W.D. Eggers, R. Hamill, A. Ali (2013), *Data as currency. Government's role in facilitating the exchange*, in "Deloitte Review", 2013, n. 13, pp. 19-31

G. Esperti (2024), *Cosa sappiamo sulla strategia italiana sull'intelligenza artificiale*, in "Wired", 12 marzo 2024

F. Faini (2020), *Il diritto nella tecnica: tecnologie emergenti e nuove forme di regolazione*, in "federalismi.it", 2020, n. 16

C. Faralli (2019), *Diritti e nuove tecnologie*, in "Tigor. Rivista di scienze della comunicazione e di argomentazione giuridica", 2019, n. 2

G. Finocchiaro (2022), *La regolazione dell'intelligenza artificiale*, in "Rivista trimestrale di diritto pubblico", 2022, n. 4

G. Finocchiaro (2019), *Intelligenza Artificiale e protezione dei dati personali*, in "Giurisprudenza Italiana", 2019, n. 7

G. Finocchiaro (2012), *Riflessioni su diritto e tecnica*, in "Il diritto dell'informazione e dell'informatica", 2012, n. 4-5

G. Finocchiaro, O. Pollicino (2022), *La strategia europea sui dati e le divergenze con quella italiana*, in "Il Sole 24 ORE", agosto 2022

L. Floridi, J. Cowls (2019), *A unified framework of five principles for AI in society*, in "Harvard Data Science Review", vol. 1, 2019, n. 1

T.E. Frosini (2022), *L'orizzonte giuridico dell'intelligenza artificiale*, in "Il Diritto dell'informazione e dell'informatica", 2022, n. 1

Garante per la protezione dei dati personali (2024), *Segnalazione al Parlamento e al Governo sull'Autorità per l'I.A.*, 25 marzo 2024

Garante per la protezione dei dati personali (2022), *Memoria del Garante per la protezione dei dati personali – COM 2021(206) Proposta di regolamento (UE) sull'intelligenza artificiale*, Camera dei Deputati – Commissioni IX e X riunite, 9 marzo 2022

D. Iacovelli, M. Fontana (2022), *Nuove sfide della tecnologia e gestione dei rischi nella proposta di regolamento europeo sull'intelligenza artificiale: set di training, algoritmi e qualificazione dei dati. Profili critici*, in "Il diritto dell'economia", 2022, n. 3

A. Mantelero (2022), *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI*, vol. 36, Springer, 2022

A. Mantelero, D. Poletti (a cura di) (2018), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna, Studi in tema di Internet Ecosystem*, Pisa University Press, 2018

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

N. Miniscalco (2020), *Il diritto alla protezione dei dati personali al tempo della mobilità intelligente*, in "Forum di Quaderni Costituzionali", 2020, n. 1

C. Napoli (2020), *Algoritmi, intelligenza artificiale e formazione della volontà pubblica: la decisione amministrativa e quella giudiziaria*, in "Rivista AIC", 2020, n. 3

C. Novelli (2024), *L'Artificial Intelligence Act Europeo: alcune questioni di implementazione*, in "federalismi.it", 2024, n. 2

OECD (2019), *Artificial Intelligence in Society*, OECD Publishing, 11 June 2019

F. Pacileo (2022), *L'intelligenza artificiale nel prisma dell'impresa: evoluzione normativa e prospettive di studio*, in "Annuario 2022. Osservatorio Giuridico sulla Innovazione Digitale", Sapienza Università Editrice, 2022

U. Pagallo (2017), *Intelligenza Artificiale e diritto. Linee guida per un oculato intervento normativo*, in "Sistemi intelligenti", 2017, n. 3, pp. 615-636

A. Pajno, M. Bassini, G. De Gregorio et al. (2019), *AI: profili giuridici Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in "BioLaw Journal – Rivista di BioDiritto", 2019, n. 3

L. Parona (2020), *Prospettive europee e internazionali di regolazione dell'intelligenza artificiale tra principi etici, soft law e self-regulation*, in "Rivista della Regolazione dei mercati", 2020, n. 1

M.G. Peluso (2023), *Intelligenza artificiale e tutela dei dati. Prospettive critiche e possibili benefici per una governance efficace*, Giuffrè, 2023

O. Pollicino, M. Bassini (2017), *Art. 8. Protezione dei dati personali*, in R. Mastroianni, O. Pollicino, S. Allegrezza et al. (a cura di), "Carta dei diritti fondamentali dell'Unione europea", Giuffrè, 2017

E.C. Raffiotta (2023), *Dalla* self-regulation *alla* over-regulation *in ambito digitale: come (e perché) di un necessario cambio di prospettiva*, in "Osservatorio sulle Fonti", 2023, n. 2

G. Resta (2022), *Cosa c'è di "europeo" nella proposta di regolamento UE sull'intelligenza artificiale?*, in "Il Diritto dell'informazione e dell'informatica", 2022, n. 2

H. Roberts, J. Cowls, J. Morley et al. (2021), *The Chinese Approach to AI: An Analysis of Policy, Ethics, and Regulation*, in "AI and Society", vol. 36, 2021

M.U. Scherer (2016), *Regulating artificial intelligence systems: risks, challenges, competencies, and strategies*, in "Harvard Journal of Law & Technology", vol. 29, 2016, n. 2

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

S. Torreggiani (2021), *La circolazione dei dati secondo l'ordinamento giuridico europeo. Il rischio dell'ipertrofia normativa*, in "Rivista italiana di informatica e diritto", 2021, n. 1

M. Valdés Borruey, L. M. Latasa Vassallo, M. Ñíguez Olalla (2023), *Spain: Agency for the supervision of AI – overview*, in "Data Guidance", November 2023

M. Veale, K. Matus, R. Gorwa (2023), *AI and Global Governance: Modalities, Rationales, Tensions*, in "Annual Review of Law and Social Science", 2023, n. 19

R. van den Hoven van Genderen (2017), *Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics*, in "European Data Protection Law Review", 2017, n. 3

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0135 • articolo sottoposto a peer review • pubblicato in anteprima il 25 mar. 2024

Vilard Bytyqi

The role of law enforcement agencies in fighting cybercrime in Kosovo: The need to adapt to new trends

Dealing with threats and real risks to cybersecurity that are produced by cybercrime necessarily imposes the construction of a strategic approach at the national and cross-national levels. Despite the fact that Kosovo has built strategies for dealing with cybersecurity, there is still no accurate data regarding the ability of institutional mechanisms to respond in a proportional and effective manner to cybersecurity threats posed by cybercrime. This paper highlights the strategic treatment of cybersecurity and cybercrime, namely the strategic objectives and activities for their fulfillment, as well as critically analyzing the legal rules that are applied in the context of preventing and fighting cybercrime, focusing on the role, responsibilities, and functions of law enforcement agencies for preventing and fighting cybercrime. This paper also analyzes the strategic objectives and the action plan envisaged by the National Cybersecurity Strategy 2023-2027, which for the first time gives special importance to the inclusion of the private sector in the national network to protect against cyber attacks. The importance of the standards of the Budapest Convention is also addressed, and an assessment is made regarding the extent of the inclusion of these standards by the state of Kosovo.

Cybersecurity Strategy – Law Enforcement Agencies – Preventing Cybercrime – Fighting Cybercrime

Il ruolo delle forze dell'ordine nella lotta alla criminalità informatica in Kosovo: la necessità di adattarsi ai nuovi scenari

Affrontare le minacce e i rischi reali per la sicurezza informatica generati dalla criminalità informatica impone necessariamente un approccio strategico a livello nazionale e transnazionale. Nonostante il Kosovo abbia sviluppato strategie per affrontare la sicurezza informatica, non esistono ancora dati accurati sulla capacità dei meccanismi istituzionali di rispondere in modo proporzionale ed efficace alle minacce alla sicurezza informatica poste dalla criminalità informatica. Questo contributo si occupa del trattamento strategico della sicurezza informatica e della criminalità informatica, vale a dire degli obiettivi strategici e delle attività per il loro raggiungimento, e analizza criticamente le norme giuridiche che vengono applicate nel contesto della prevenzione e della lotta alla criminalità informatica, concentrandosi sul ruolo, sulle responsabilità e sulle funzioni delle autorità di contrasto per la prevenzione e la lotta alla criminalità informatica. Nel presente contributo vengono inoltre analizzati gli obiettivi strategici e il piano d'azione previsti dalla Strategia Nazionale di Cybersecurity 2023-2027 che, per la prima volta, attribuisce particolare importanza all'inclusione del settore privato nella rete nazionale per la protezione dagli attacchi informatici. Viene inoltre affrontata l'importanza delle norme della Convenzione di Budapest e viene valutata la portata dell'inclusione di tali norme da parte dello Stato del Kosovo.

Strategia per la cibersicurezza – Autorità di contrasto – Prevenzione della criminalità cibernetica Contrasto alla criminalità cibernetica

The Author is associate professor at the Faculty of Public Safety, at the Kosovo Academy for Public Safety. He is a member of the Kosovo Judicial Council and a trainer at the Academy of Justice

1. Introduction

The approach to cybersecurity, with special emphasis on cybercrime as one of the main cybersecurity threats, requires extensive institutional measures, including clear strategies, appropriate legal rules, clearly defining the roles of institutional mechanisms, and dedicating sufficient resources and professionally prepared officials to meet the objectives for maintaining and advancing cybersecurity.

Concerns about cyber threats have been expressed at various levels: international, regional, and national. This issue has received serious and extensive treatment on the European level, where Kosovo is also a political and geographical part, since cybercrime is considered one of the main issues by the EU authorities in the context of cybersecurity[1]. The treatment of cybercrime at the international level has received a lot of attention when it is known that all countries are affected by this contemporary form of criminality, which is reflected by international initiatives that aim to build a common approach to this form of criminality that is also threatening international security. One of these initiatives is the drafting of the Convention on Cybercrime, which recognizes the need to pursue a common criminal policy as a priority and aims to protect society from cybercrime, among other things, by drafting appropriate legislation and promoting international cooperation in this field[2]. Cybersecurity requires coherent and detailed strategic planning, appropriate legal regulation, and other related measures. Recently, countries around the world have increasingly focused on drafting new laws and other documents, as well as adopting or updating national cybersecurity strategies. Currently, most countries have adopted effective national cybersecurity strategies. The adoption of cybersecurity strategies has been particularly high since 2011[3].

National strategies emphasize the necessity of drafting and effective implementation of legislation in the fight against cybercrime. In this regard, regardless of the design of strategies for cybersecurity and cybercrime or even the design of the criminal legal framework in this area, an important aspect that produces concrete results from the implementation of the law and from the fulfillment of strategic responsibilities remains the role of enforcement agencies of the law, which with their capacities respond to cybersecurity threats. The State Strategy for Cybersecurity is one of the most important documents that deals with cybersecurity and defines the role of law enforcement institutions and agencies in relation to cybersecurity, which is threatened by cybercrime.

This paper first examines the strategic documents and the criminal legal framework for cybersecurity, as well as their compatibility with the standards of international instruments, and shows the need for necessary improvements in the parts where it is estimated that improvements are needed. Then, it examines the need for the design of a new strategy for cybersecurity and analyzes the need that the new strategy must be harmonized

1. Štitilis-Pakutinskas-Malinauskaitė 2017.
2. Council of Europe 2002.
3. Štitilis-Pakutinskas-Laurinaitis-Malinauskaitė 2017, pp. 357-372.

with the standards and guidelines for effective strategies, including, among other things, the need to include the Convention on Cybercrime and other important international instruments in this field. Also, the role, importance, and responsibilities of law enforcement agencies that have a legal mandate to deal with cybercrime prevention and combat are discussed. Among others, the responsibilities of the Information Society Agency, the Kosovo Intelligence Agency, the police, the prosecution, courts, and other law enforcement institutions and agencies are addressed.

2. The Cybersecurity Strategy

Due to the danger posed by cybercrime for internal and international security, this issue is now being dealt with strategically by all countries. This is also observed by international, regional, and global initiatives where the issue of addressing cybercrime is expressed more and more every day. The importance of treating this issue as an area of common international interest is also expressed by the Resolution of the European Parliament of 2013 on the Cybersecurity Strategy of the European Union, where it is emphasized that criminal activities in cyberspace can be equally harmful to the well-being of societies as violations in the physical world and that these forms of crime often reinforce each other, as can be seen, for example, in the sexual exploitation of children, organized crime, and money laundering[4].

Kosovo has drafted and approved the State Strategy for Cybersecurity 2016-2019, becoming one of the first countries in the Western Balkans after Montenegro to draft and approve a strategy in this field[5]. The State Strategy for Cybersecurity has been drafted based on assessments and analyses of the needs of law enforcement agencies, government institutions, local and international organizations, global trends, as well as practices and policies of the European Union. In this context, the strategy is in full harmony with the guidelines of the European Union Agency for Cybersecurity and the strategies of several EU Member States. All state institutions, professional associations, the private sector, civil society, and international partners were included in the working group for the drafting of this document[6].

In terms of structure, this document contains the general principles, legal framework and institutional mechanisms, objectives, system of implementation, monitoring and evaluation of implementation, as well as an action plan. The objectives of the cybersecurity strategy are described in the sixth part of this document and include:

a) protection of critical information infrastructure;
b) development of the institutional and legal framework as well as the development of human and technical capacities;
c) construction of a public-private partnership;
d) reaction to incidents;
e) international cooperation.

The strategy foresees the institutional mechanisms that have a role and importance in cybersecurity and have a mandate for the design and implementation of state policies in this field[7]. This document addresses the responsibilities of institutions and law enforcement agencies in the field of cybercrime and cybersecurity in accordance with their legal mandate and foresees that this strategy has the coordination of the Ministry of Internal Affairs or one of his authorized representatives. In this regard, some states are now re-examining the issue of policy formulation and implementation at a higher state and more professional level; e.g., Germany, Japan and the Netherlands plan a strategic-level cybersecurity council[8].

In this strategy, dealing with cybercrime does not receive much attention, as the entire focus of this document is on strengthening capacities for cybersecurity. Cybercrime draws attention to the part of the legal infrastructure where it is foreseen

4. Joint communication to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *Cyber security strategy of the European Union: an open, safe and secure cyberspace*, JOIN/2013/01, Brussels 7 February 2013.
5. Kosovar Center for Security Studies 2022.
6. Ministry of Internal Affairs 2015.
7. *Ibid*.
8. Luiijf-Besseling-Spoelstra-De Graaf 2013.

that the law on the prevention and combating of cybercrime should be reviewed based on modern trends to respond to this form of crime. Meanwhile, special care has been devoted to the advancement of the technical infrastructure with the aim of advancing the equipment for the investigation of cybercrime[9]. In the same way as Kosovo, the national cybersecurity strategies of many countries do not directly mention the fight against cybercrime or reducing the number of cybercrimes. However, there are also countries that reserve a separate chapter for the treatment of cybercrime[10]. Even in the document published by the Global Cybersecurity Capacity Center[11], it is emphasized that Kosovo still does not have any cybersecurity command and control centers at the national level. Although the Kosovo Security Force and Police have cybercrime units, their capacities are severely limited due to a lack of human resources.

Even though this document is intended to revise the Law on the Prevention and Fight Against Cybercrime, this process has never been completed, which is why the legal rules applicable to the prevention and fight against cybercrime have not been updated and adapted to the trends of cybercrime, which, as a form of crime, stands out for the fast dynamics of its development. The field of cybernetics is regulated by several legal acts that are approved by the Assembly of Kosovo, including here, *Law on Information Society Government Bodies*[12]; *Law on the Information Society Services*;[13] *Law on Electronic Communications*[14]; *Law on Interception of Electronic Communications*[15]; as well as the *Law on Protection of Personal Data*[16].

3. The role of law enforcement agencies in preventing cybercrime

Building a proper approach to cybercrime prevention is a rather complex issue. In addition to the general approach to crime prevention that is known in the theories of crime prevention, in the cybercrime prevention strategy, some other approaches are also used that adapt to the specifics that characterize this particular form of criminality. In this regard, genuine criminal investigations allow us to understand the modus operandi used by persons involved in cybercrime as perpetrators of criminal offences. A broad understanding of modus operandi can be used by law enforcement agency officials to design and implement cybercrime prevention policies. Also, intelligence and strategic analysis are vital in the fight against cybercrime. Europol recently adopted a very well-structured strategic analysis methodology in the framework of Serious and Organized Crime Threat Assessment (SOCTA). Such a methodology, generally built to analyze the threat posed by serious organized groups, can be used, mutatis mutandis, to examine the specifics of cybercrime threats[17].

Based on the legal and strategic framework applicable in Kosovo, in the following we will reflect on the institutions and law enforcement agencies that have in their scope the prevention of crime, including cybercrime.

At the strategic level, the Ministry of Internal Affairs is the central authority that coordinates activities with all institutions and law enforcement agencies in the field of cybersecurity and has the obligation to monitor the implementation of the strategy and the fulfillment of strategic objectives.

9. Ministry of Internal Affairs 2015.
10. Štitilis-Pakutinskas-Malinauskaitė 2017.
11. Bada 2015.
12. *Law on Information Society Government Bodies*, Official Gazette of the Republic of Kosovo, No. 15/2013, 15 May 2013, Law No. 04/L-145.
13. *Law on the Information Society Services*, Official Gazette of the Republic of Kosovo, No. 6/2012, 11 April 2012, Law No. 04/L-094.
14. *Law on Electronic Communications*, Official Gazette of the Republic of Kosovo, No. 30/2012, 9 November 2012, Law No. 04/L-109.
15. *Law on Interception of Electronic Communications*, Official Gazette of the Republic of Kosovo, No. 18/2015, 13 July 2015, Law No. 05/L-030.
16. *Law on Protection of Personal Data*, Official Gazette of the Republic of Kosovo, No. 6/2019, 25 February 2019, Law No. 06/L-082.
17. Buono 2014.

For this purpose, at the level of this institution, the Secretariat of Strategies functions as a permanent body that has a mandate for all strategic documents issued by the Government of Kosovo. The Information Society Agency was established by the Law on Information Society Government Bodies and serves as the central body of the state administration for the development and implementation of information and communication technology for the institutions of the Republic of Kosovo (Article 5)[18]. Also, as needed, the Information Society Agency helps the relevant institutions in the fight against cybercrime and ensures the protection of personal data in electronic form in accordance with the legislation in force[19].

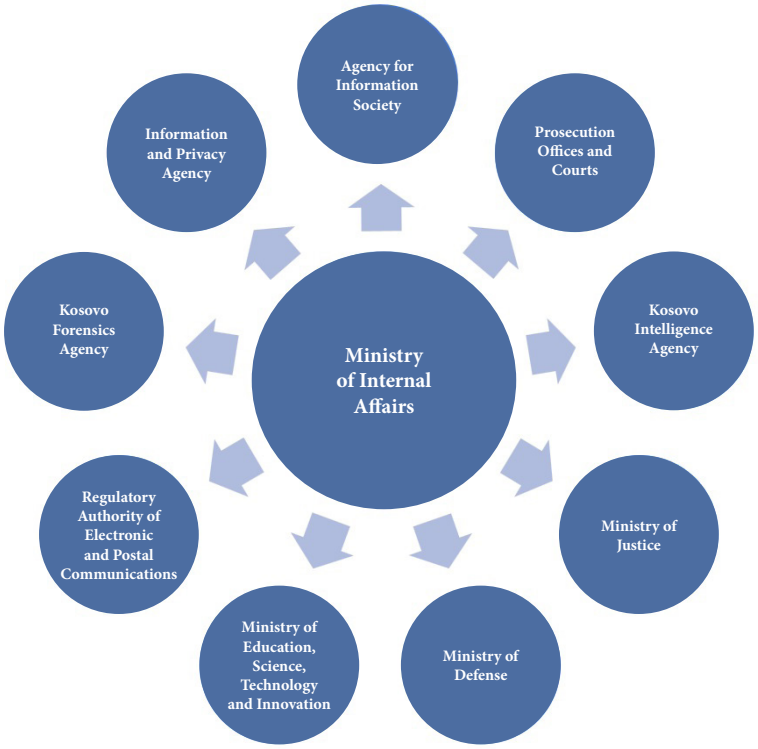


Fig. 1 — *Institutions and law enforcement agencies that have a mandate to prevent cybercrime* [Ministry of Internal Affairs 2023]

An important function for the identification and detection of potential threats that endanger cybersecurity is also played by the Kosovo Intelligence Agency, which, within its constitutional and legal mandate, has the authority to collect information about threats to the security of Kosovo, which includes the collection of intelligence information for the purposes of cybersecurity protection[20]. The role of the Kosovo Intelligence Agency as a national security institution is not clearly defined by the State Strategy for Cybersecurity 2016-2019. In addition to the activity that is foreseen by the Action Plan of this strategy for the advancement of regional and international cooperation in the fight against cybercrime that is determined to be fulfilled together with some other law enforcement authorities, the specific tasks related to the fulfillment of any specific task are not highlighted in this document; therefore, the commitment of the Kosovo Intelligence Agency remains unclear for the implementation of this strategy.

On the other hand, the police, as an agency within the Ministry of Internal Affairs, play an important role in preventing crime in general, including taking measures to prevent cybercrime. This duty is provided in Article 10 of the *Law on Police*[21], as one of the general duties of the police, which, among other things, provides for the prevention of danger to citizens and to maintain order and public safety, as well as to prevent and detect criminal offences and their perpetrators, including taking proactive actions to prevent cybercrime.

To fulfill its legal mandate, the issue of police crime control involving digital technology and

18. *Law on Information Society Government Bodies*, Official Gazette of the Republic of Kosovo, No. 15/2013, 15 May 2013, Law No. 04/L-145.
19. Ministry of Internal Affairs 2015.
20. *Law on the Kosovo Intelligence Agency*, Official Gazette of the Republic of Kosovo, No. 30/2008, 15 June 2008, Law No. 03/L-063.
21. *Law on Police*, Official Gazette of the Republic of Kosovo No. 4/2012, 19 March 2012, Law No. 04/L-076.

computer networks also requires a range of new collaborations, including collaboration between the police and other agencies, collaboration between the police and private institutions, and collaboration between the police of at least two states, namely the creation and advancement of international cooperation, which can be done through permanent mechanisms that have already been established or even through direct relations between the police[22]. Considerable progress has been made over a period of time in building the capacity of the national police to respond to cybercrime, and there is now a growing awareness among computer users of the need for basic Internet security[23].

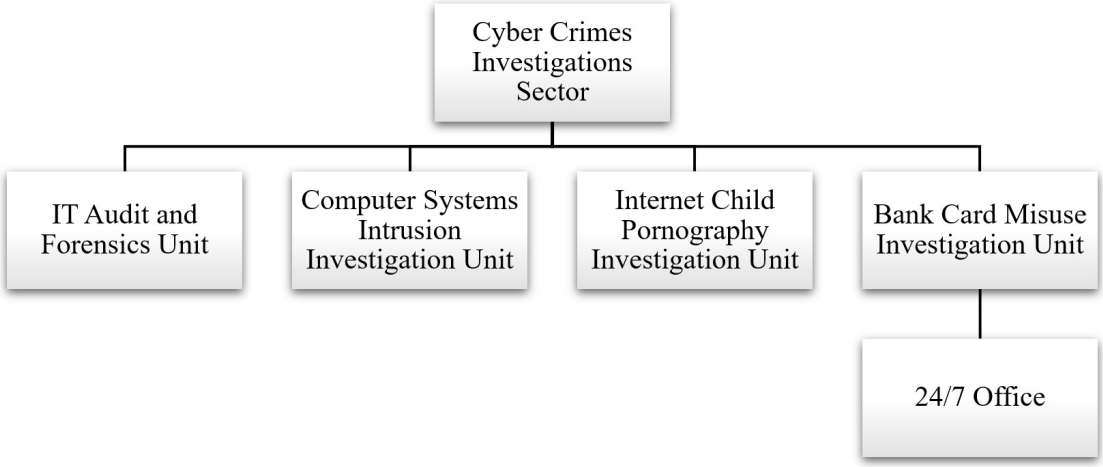


Fig. 2 — *The organizational structure of the Cybercrime Investigations Sector* [Kosovo Police 2019]

An important role in the prevention of cybercrime in the institutional structure is also exercised by other institutional mechanisms which are defined according to the Law on Electronic Communications, Law on Protection of Personal Data, as well as other laws.

4. The role of law enforcement agencies in fighting cybercrime

Depending on national specifics, states are organized differently to investigate and prosecute cybercrime; e.g., the United Kingdom, due to the specifics of its internal organization, addresses the issue of investigation and criminal prosecution through many central and local institutional mechanisms that are specialized in dealing with cybercrime[24]. In many countries around the world, law enforcement agencies have developed specialized units[25]. While in Kosovo, the primary responsibility for the investigation and documentation of criminal offences in the field of cybernetics is with the police, other law enforcement agencies are involved in the investigation of these criminal offences when it is necessary to build joint investigative groups or the criminal case falls directly under the legal responsibilities that these agencies have. The concentration of resources in only one agency is due to the possibility of more effective criminal investigation and prosecution, but also due to the low rate of presentation of criminal offences for which the state must have the capacity to respond. Focusing only on one state agency for the investigation of these crimes can be found in many small countries; e.g., Iceland is one such example where the criminal investigation is concentrated only in the capital[26].

In Kosovo, the procedure for investigating criminal offences is regulated according to the

22. Broadhurst 2006.
23. *Ibid.*
24. Bada-Arreguin-Toft-Brown et al. 2016.
25. Brown 2015.
26. Bada-Arreguin-Toft-Brown et al. 2016.

Code of Criminal Procedure, where it is determined that initial police actions are the responsibility of law enforcement agencies that have police

Agency	Law	Scope
The Tax Administration of Kosovo	Law No. 03/L-222 on Tax Administration and Procedures	Art. 75 (1)
Customs	Code No. 03/L-109 Customs and Excise Code of Kosovo	Art. 302 (1)
Police Inspectorate of Kosovo	Law No. 03/L-23 on Police Inspectorate of Kosovo	Art. 2 (1) (1)
Financial Intelligence Unit of the Republic of Kosovo	Law No. 05/L-096 on the Prevention of Money Laundering and Combating Terrorist Financing	Art. 4 (1)

Tab. 1 — *Law enforcement agencies that have police powers in Kosovo*

authorizations[27]. The Code of Criminal Procedure does not explicitly define the law enforcement agencies that have police powers, as this issue is dealt with by separate laws that regulate the scope of these agencies. According to special laws, in addition to the police, there are also several other law enforcement agencies that have police authorizations, listed in table 1.

These agencies can act independently when the criminal investigation of cybercrime cases is within their mandate defined by law and does not relate to the scope of other law enforcement agencies. These law enforcement agencies operate under the authority of the State Prosecutor.

Depending on the scope and complexity of the crime, several law enforcement agencies may jointly investigate a complex criminal case, including cybercrime. The joint investigation comes into expression even when cybercrime has such an extent that it violates the laws of at least two countries, which has international elements, and there is a need to develop joint procedures for the investigation of these criminal offences. This activity can be facilitated by international instruments for international legal cooperation as well as direct agreements concluded between states. The traditional mechanisms of criminal investigation and prosecution have been assessed as insufficient to combat serious cross-border crime, including cybercrime that operates in a virtual world with the possibility of taking actions and causing consequences in an unpredictable manner. Therefore, it has been estimated that the creation of a joint team of two or more states would effectively improve crime with an international element. Investigations would be coordinated, while prosecutors would directly access relevant information from different countries[28].

Within the police organization, the Department of Investigation functions as one of the three main pillars that make up the high structure of the internal organization of this agency[29]. This pillar also deals with the aspect of criminal offences in the field of cybernetics since the Directorate Against Organized Crime functions as a separate unit within its hierarchy and has the Cybercrime Investigation Sector. The scope of this unit is related to serious criminal offences for which in-depth investigation and special expertise are required, since other criminal offences from the field of cybernetics can also be investigated by non-specialized units that operate within the police stations that deal with crime generally.

27. *Criminal Procedure Code*, Official Gazette of the Republic of Kosovo, No. 24/2022, 17 August 2022, Code No. 08/L-032.
28. Deutsche Gesellschaft für Internationale Zusammenarbeit 2014.
29. *Law on Police*, Official Gazette of the Republic of Kosovo No. 4/2012, 19 March 2012, Law No. 04/L-076.

According to the organizational structure, five units operate in the Cybercrime Investigation Sector, namely the IT Control and Forensics Unit, the Computer Systems Intrusion Investigation Unit, the Internet Child Pornography Investigation Unit, the Card Abuse Investigation Unit, and Banking and Office 24/7[30]. The 24/7 Office is a mechanism envisaged by the Convention on Cybercrime of the Council of Europe as a point of contact available twenty-four hours a day, seven days a week, in order to ensure the provision of immediate assistance for the purposes of investigations or procedures related to criminal offences related to computer systems and data or to the collection of evidence in electronic form related to the criminal offence. The Convention on Cybercrime provides for the 24/7 clause to expedite and, in some cases, act as competent authority when urgent action is required on certain issues[31]. Precisely for this purpose, the 24/7 Office that operates within the Cybercrime Investigations Sector aims to play the role that the Convention on Cybercrime provides for quick actions related to cybercrime issues or other issues related to this field.

In the fight against cybercrime, the police is challenged by many issues, especially: number of users, the availability of tools and information, difficulties in tracing offenders, missing mechanisms of control, the absence of borders in cyberspace and the international component of cybercrime. Not only is the complexity of investigating cybercrimes, but cyber policing in general tends to be hampered. It is very difficult for police units to initiate investigations due to the invisibility of such crimes and lack of reporting[32].

The State Prosecutor is responsible for the prosecution of persons suspected of these criminal offences[33]. The State Prosecutor still does not have any special units or specialized prosecutors that would specifically deal with the prosecution of these criminal offences. Also, the courts do not have any special departments that judge criminal offences in this field. All courts of first instance have the competence to deal with these criminal offences, as provided by the Law on Courts[34]. Also at the appeal level, the judicial system does not have any specialized department that will deal with this category of criminal offences. In addition to the lack of specialization at the institutional level, there is also a lack of specialization among judges, since they deal with all criminal cases that fall under the competence of the department where they serve. The importance of the specialization of courts and judges for specific cases, including the field of cybercrimes, is manifold, since the judges who deal with these cases have relevant professional expertise, but the courts are also more efficient[35].

Although there are no prosecutors and judges who will deal only with these criminal offences, specialized trainings related to the field of cybercrime are organized. This is also reflected in the annual programs organized by the Academy of Law, where cybercrime training is foreseen, namely several training sessions for judges and prosecutors who deal with cybercrime issues[36].

5. The need to adapt to new trends

Even though the duration of the State Strategy for Cybersecurity was valid only for the period 2016–2019, the document for the new strategy is in the drafting phase by the Ministry of Internal Affairs and is now open to public consultation. The lack of a workable document that deals with cybersecurity from a strategic point of view has created a vacuum for dealing with the problem from a strategic perspective, even worse when it is known that a front of multi-disciplinary mechanisms must be built to approach the problem of cybercrime and cybersecurity, which is now one of the most serious threats to not only national but also international security. The national cybersecurity strategy, as a strategic document, should be one of the es-

30. *Ibid.*
31. Council of Europe 2002.
32. Tropina 2017.
33. Sahiti-Murati-Elshani 2014.
34. *Law on Courts*, Official Gazette of the Republic of Kosovo, No. 22/2018, 18 December 2018, Law No. 06/L–054.
35. Wasserman-Slack 2021.
36. Academy of Justice 2023.

sential documents in every state that provides the basics and measures to guarantee cybersecurity, as well as the priorities for its improvement[37].

The importance of dealing with this issue in a strategic aspect is proven by the treatment of cybercrime and cybersecurity in the Security Strategy of Kosovo, where cybercrime and cybersecurity are identified as issues that constitute one of the challenges that the global security environment faces today, where Kosovo is also exposed to hybrid threats, which include non-conventional, foreseen with the Security Strategy and Cybersecurity Strategy (2016-2019) were insufficient to include the private sector, which is one of the most sensitive areas exposed to threats from cybercrime. In the National Cybersecurity Strategy 2023-2027, for the first time as a special objective, «Advancement of investigative and military cybersecurity capabilities» is envisaged. One of the concrete measures related to the fulfillment of this objective is the advancement of legislation; collecting accurate and reliable statistics; increasing the number

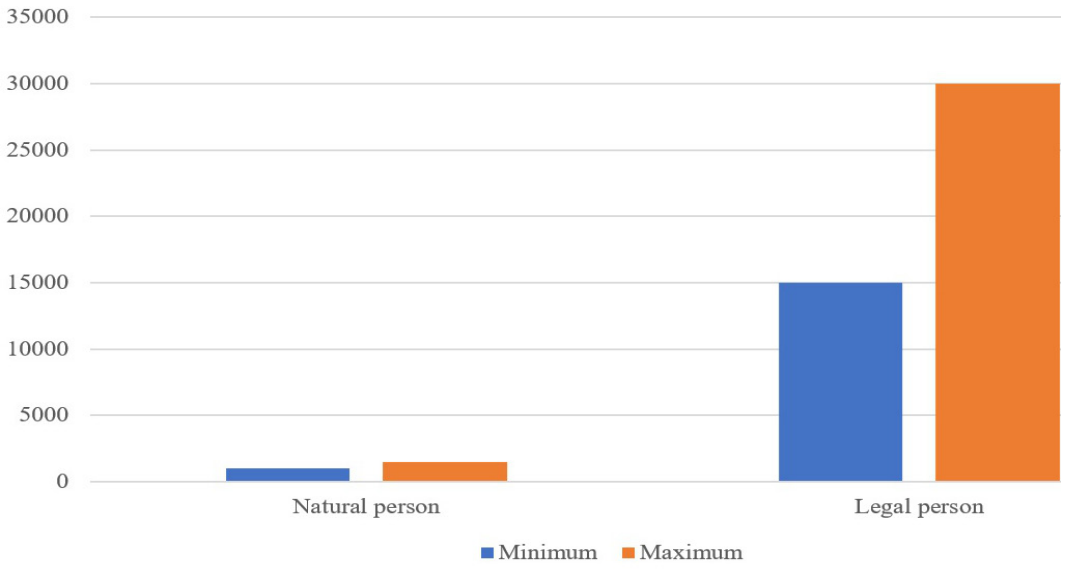


Fig. 3 — *Minor offence sanctions*

asymmetric elements that influence extension operations and cyber attacks that aim to weaken the country's sovereignty, undermine the country's integrity, and damage the country's image in the international arena[38].

National Cybersecurity Strategy 2023-2027 presents a more advanced document that includes the most important aspects that a strategic document should contain. Unlike the previous strategy, this document contains aspects that are addressed for the first time, with special emphasis on the treatment and protection from cyber threats of the non-state sector as well. Such a strategic approach fills the former and current vacuum on this issue. The strategic institutional mechanisms that were of law enforcement officials in the police, prosecutor's office, and courts; and engaging experts from the private sector. The activities planned for this strategic objective will be classified and not made public.[39]

At the international level, guidelines have already been drawn up for the drafting of these strategic documents that will help the states build effective strategies at the domestic level. One of them is the Guide to Developing a National Cybersecurity Strategy, where this document provides some good practices that states should adapt in their national documents, including governance, risk management in national cybersecurity, preparedness and resilience, critical infrastructure services and

37. Štitilis-Pakutinskas-Laurinaitis-Malinauskaitė 2017.
38. Government of Kosovo 2022.
39. Ministry of Internal Affairs 2023.

essential services, capability and capacity building and awareness raising, legislation and regulation, and international cooperation.[40]

In addition to addressing cybercrime and cybersecurity in terms of strategic documents, a number of legal initiatives have been undertaken to address cybercrime and cybersecurity. One of them is the initiative of the government to sponsor the Law on Cybersecurity, which has already passed the institutional filters, starting from the Ministry of Internal Affairs and the government, and has been approved by the Assembly of Kosovo. This law defines the principles of cybersecurity, the institutions and agencies that develop and implement the cybersecurity policy, the responsibilities of the authorities in the field of cybersecurity, the duties of cybersecurity entities, inter-institutional cooperation, as well as the prevention of cyber attacks in the Republic of Kosovo. With this law, the Cybersecurity Agency is established for the first time[41]. The Agency for Cybersecurity will have primary responsibility for the implementation of this law and will act under the authority of the Ministry of Internal Affairs. It will also have the authority to coordinate activities relevant to the fulfillment of the cybersecurity mission with all parties involved in cybersecurity, inside and outside Kosovo.

In this law, it is foreseen that in some parts the Law on Prevention and Fight of Cybercrime[42] will be supplemented or amended, as it is planned that some legal provisions of this law will be repealed, namely Article 5 in its entirety (prevention, security, and informative campaigns), Article 6 (maintenance, completion, and use of the database), Article 7 (training and special programs), and Article 8 (obligations of owners and administrators)[43]. This law partially transposes Directive 2013/40/EU[44] of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, as well as Directive (EU) 2016/1148[45] of 6 July 2016 concerning measures for a high common level of security of networks and information systems across the Union.

According to Article 3 of the law, the expressions "operator of essential services" and "provider of digital services" are defined. According to the law, the expression "operator of essential services" means a public or private entity that possesses national critical infrastructure according to the respective Law on Critical Infrastructure (Art. 3 (1)(12)). While the expression "Digital service provider" means a legal person with a base or branch registered in the Republic of Kosovo that provides digital services (Art. 3 (1)(13)). This definition is harmonized with points (4) and (6) of Article 4 of Directive (EU) 2016/1148.

The law provides a separate chapter for obligations to guarantee cybersecurity. In this regard, the operator of essential services must permanently implement organizational security measures as well as determine if any cyber incident has occurred that has a significant impact on system security or service continuity (Article 5 and Article 6)[46]. Also, the provider of digital services is required to ascertain the risks that affect the security of their system, analyze them, and take adequate organizational and technical measures for risk management. The digital service provider must notify the Cybersecurity Agency of a cyber incident that has a significant impact on the digital service provided immediately after becoming aware of the cyber incident (Article 7 and Article 8). The law foresees

40. International Telecommunication Union 2018.
41. *Law on Cybersecurity*, Official Gazette of the Republic of Kosovo, No. 4/2023, 22 February 2023, Law No. 08/L-173.
42. *Law on Prevention and Fight of the Cyber Crime*, Official Gazette of the Republic of Kosovo, No. 74/2010, 20 July 2010, Law No. 03/L-166.
43. L*aw on Cybersecurity*, Official Gazette of the Republic of Kosovo, No. 4/2023, 22 February 2023, Law No. 08/L-173.
44. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.
45. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
46. *Law on Cybersecurity*, Official Gazette of the Republic of Kosovo, No. 4/2023, 22 February 2023, Law No. 08/L-73.

the possibility of imposing criminal sanctions if it is estimated that operators of essential services and providers of digital services do not take the measures defined in Articles 5, 6, 7, and 8 of this law[47]. The law foresees the possibility of imposing criminal sanctions (fines) against legal persons and natural persons.

The Law on Cybersecurity foresees minor offence sanctions, namely higher fines for legal entities while lower fines are provided for natural persons. This law does not foresee any criminal offence for violating its legal provisions. In this regard, this law only provides for minor offence sanctions that are imposed in administrative procedure by the relevant authorities.

Despite the effort to advance the regulation of this field with effective laws, there is still a lack of concrete implementation of the provisions contained in the Convention on Cybercrime, known as the Budapest Convention. The primary purpose of this instrument is to advance and fulfill the objectives for preventing and fighting cybercrime at the national level, with the aim of producing results at the international level as well. This is also reflected in the goals of this instrument, which can be summarized as follows: 1) harmonization of domestic material criminal laws in the field of cybercrime; 2) ensuring the necessary legal powers of the criminal procedure for the investigation and prosecution of such crimes; and 3) creating a fast and effective international cooperation mechanism[48].

The Convention on Cybercrime aimed to establish an important basis of cooperation between states, creating an important reference in terms of content, but it also aimed to unify the rules between states, which is reflected in the fact that this instrument, although it was sponsored by the Council of Europe, remains open for ratification by other countries that are not members of this international organization. This is proven by the large number of countries that are not members of the Council of Europe; an example is the USA, but there are also other countries. Now this instrument has 67 party states, of which 1 third are not members of the Council of Europe.

6. Conclusion

The State Strategy for Cybersecurity is one of the most important documents that deals with cybersecurity and defines the role of law enforcement institutions and agencies in relation to cybersecurity, which is threatened by cybercrime. The State Strategy for Cybersecurity of Kosovo was one of the first documents approved in this field in the Western Balkans. The strategy foresees the institutional mechanisms that have a role and importance in cybersecurity, and these institutional mechanisms have a mandate for the design and implementation of state policies in this field. In the strategy implemented during the period 2016-2019, the treatment of cybercrime does not receive much attention, as the focus is on strengthening capacities for cybersecurity.

A number of important legal initiatives have been undertaken that focus on dealing with cybersecurity and cybercrime. One of these initiatives is the government's initiative to sponsor the Law on Cybersecurity, which has already passed the institutional filters and been approved by the Assembly of Kosovo. The field of cybernetics is regulated by several legal acts issued by the Assembly of Kosovo, including the Law on Information Society Government Bodies, the Law on Information Society Services, the Law on Electronic Communications, the Law on Interception of Electronic Communications, and the Law on Protection of Personal Data. Regarding the functions performed by law enforcement agencies for the prevention and combating of cybercrime, there is no special treatment from a strategic point of view, even though this part is very important and stands out from many international instruments in this field.

Regarding the fight against cybercrime, the police have the primary responsibility for investigating and documenting criminal offences in the field of cybernetics, while other law enforcement agencies are involved in the investigation of cybercrime when necessary. The procedure for the investigation of criminal offences is regulated according to the Code of Criminal Procedure, which states that initial police actions are the responsibility of law enforcement agencies that have police authorizations.

47. *Ibid.*
48. Brenner 2007.

Within the police, there is a special unit that deals with cybercrime, while the prosecution and courts do not have any specialized departments that specifically deal with this category of criminal offences.

National Cybersecurity Strategy 2023-2027 presents an advanced document that includes the most important components that a strategic document should contain. This document is the continuation of the previous strategy in this area. Unlike the previous strategy, this document is more advanced and contains components that are included for the first time, with special emphasis on the treatment and protection from cyber threats of the non-state sector as well. The issue of cybercrime investigations is also dealt with in detail and is detailed in an important way in the action plan of this document. Despite the advancement of the strategic and legal framework in the field of cybersecurity and cybercrime, the full transposition of the rules and standards contained in the Budapest Convention has not yet been done.

References

Academy of Justice (2023), *Training Program 2023*, Prishtina, 2023

M. Bada (2015), *Cyber security Capacity Assessment of the Republic of Kosovo*, Global Cyber Security Capacity Centre, 2015

M. Bada, I. Arreguin-Toft, I. Brown et al. (2016), *Cyber security Capacity Review of the United Kingdom*, Global Cyber Security Capacity Centre, University of Oxford, 2016

S.W. Brenner (2007), *Cybercrime: Re-Thinking Crime Control Strategies*, in Y. Jewkes (ed.), "Crime Online", Willan, 2007

R. Broadhurst (2006), *Developments in the global law enforcement of cyber-crime*, in "Policing: An International Journal", vol. 29, 2006, n. 3

C.S.D. Brown (2015), *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*, in "International Journal of Cyber Criminology", vol. 9, 2015, n. 1

L. Buono (2014), *Fighting cybercrime through prevention, outreach and awareness raising*, in "ERA Forum. Journal of the Academy of European Law", vol. 15, 2014, n. 3

Council of Europe (2002), *Convention on Cybercrime,* Budapest, 23 November 2001, Council of Europe Publishing, 2002

Deutsche Gesellschaft für Internationale Zusammenarbeit, *The fight against organized crime and corruption: Strengthening the Network of Prosecutors*, Sarajevo, 2014

Government of Kosovo (2022), *Kosovo Security Strategy 2022-2027*, Prishtina, 2022

Kosovar Center for Security Studies (2022), *Safeguarding Critical Infrastructure in Kosovo. Deconstructing Existing Policies and Practice*, Prishtina, 2022

Kosovo Police (2019), *The organizational structure of the Cybercrime Investigations Sector*, Pristina, 2019

International Telecommunication Union (2018), *Guide to Developing a National Cyber security Strategy. Strategic Engagement in Cyber security*, ITU, 2018

H.A.M. Luiijf, K. Besseling, M. Spoelstra, P. De Graaf (2013), *Ten National Cyber Security Strategies: a Comparison: Critical Information Infrastructure Security*, in S. Bologna, B. Hämmerli, D. Gritzalis, S. Wolthusen (eds.), "Critical Information Infrastructure Security", Springer, 2013

Ministry of Internal Affairs (2023), *National Cyber Security Strategy 2023-2027*, Pristina, 2023

Ministry of Internal Affairs (2015), *National Cyber Security Strategy and Action Plan 2016-2019*, 2015

E. Sahiti, R. Murati, XH. Elshani (2014), *Commentary - The Code of the Criminal Procedure*, Pristina, 2014

D. Štitilis, P. Pakutinskas, M. Laurinaitis, I. Malinauskaitė (2017), *A Model for the national cyber security strategy. The Lithuanian case*, in "Journal of security and sustainability issues", vol. 6, 2017, n. 3

D. Štitilis, P. Pakutinskas, I. Malinauskaitė (2017), *EU and NATO cyber security strategies and national cyber security strategies: a comparative analysis*, in "Security Journal", vol. 30, 2017

T. Tropina (2017), *Cyber-policing: the role of the police in fighting cybercrime*, in "European Law Enforcement Research Bulletin", 2017, n. 2

M.F. Wasserman, J.D. Slack (2021), *Can There Be Too Much Specialization? Specialization in Specialized Courts*, in "Northwestern University Law Review", vol. 115, 2021, n. 5

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0154 • articolo sottoposto a peer review • pubblicato in anteprima il 24 mag. 2024

Federica Camillieri

Rassegna sul tema dell'accesso ad Internet in carcere a livello comparato: tra riconoscimenti teorici e difficoltà pratiche

Promuovendo la premessa che l'accesso a Internet costituisce una prerogativa per lo sviluppo della persona umana, questo contributo focalizza l'attenzione su una particolare tipologia di (potenziali) utenti di Internet, e cioè le persone private della libertà, in alcuni degli ordinamenti che vedono nella risocializzazione un elemento essenziale della fase esecutiva della pena. Si considererà, tuttavia, che, laddove si riconosca una compatibilità tra la possibilità di fruire di accedere a Internet e lo stato di detenzione, si deve operare un necessario bilanciamento tra lo sviluppo della personalità umana e la sicurezza. Muovendo, quindi, dallo studio del caso italiano, sarà, poi esplorata, in primo luogo, la giurisprudenza della Corte EDU e, successivamente, la configurazione che l'accesso a Internet in carcere assume in quelle realtà statuali che declinano tale accesso come una libertà (quali il Belgio, la Spagna e la Francia) e in quelle che lo elevano a diritto sociale (come in Finlandia e Norvegia).

Accesso a Internet – Carcere – Stato di detenzione – Diritto sociale – Libertà

Review on the Topic of Internet Access in Prison on a Comparative Level: Between Theoretical Recognitions and Practical Challenges

Taking the moves from the premise that access to the Internet plays a fundamental role for the development of the human person, this study focuses on a particular category of (potential) Internet users – namely, individuals deprived of their liberty –, in the context of certain legal systems that view resocialisation as an essential element of the sentence execution phase. At the same time, where a compatibility between the possibility of accessing the web and the state of detention is to be recognized, a necessary balance must be found between the development of the human personality and security. The analysis will begin with the Italian case, then explore, firstly, the jurisprudence of the European Court of Human Rights, and, subsequently, the framework for Internet access in prison as configured in those States where such access is viewed as a freedom (such as Belgium, Spain, and France) and in those where it is elevated to a social right (such as Finland and Norway).

Internet access – Prison – State of detention – Social right – Freedom

L'Autrice è dottoranda in Scienze giuridiche, curriculum Teoria dei diritti fondamentali, giustizia costituzionale, comparazione giuridica, diritto e religione, Università di Pisa

1. Introduzione

Se, in un quadro globale, solo un numero esiguo di Costituzioni[1] prende in esame, espressamente, l'accesso a Internet nel catalogo di diritti che viene approntato, sono, invece, considerevoli le pronunce giurisprudenziali che affrontano – sulla base di differenti presupposti – la spinosa questione della natura[2] di tale accesso, sovente identificandolo come strumento di espressione di altri diritti o libertà costituzionalmente riconosciuti[3], prima tra tutti la libertà di manifestazione del pensiero nelle sue varie accezioni[4].

In sede di Nazioni Unite, si è evidenziato come Internet sia divenuto uno strumento indispensabile «per realizzare una vasta gamma di diritti umani, combattere la disuguaglianza e accelerare lo sviluppo e il progresso umano»[5], poiché «gli stessi diritti che le persone hanno *offline* devono essere tutelati anche *online*, in particolare la libertà di espressione[6]». Ciascuno Stato, quindi, dovrebbe sviluppare una politica volta a rendere Internet accessibile ed economicamente sostenibile «a tutti i segmenti della popolazione[7]».

Partendo da tali assunti, in queste pagine si focalizzerà l'attenzione su una particolare tipologia

1. Per un approfondimento sul tema, si rinvia a Passaglia 2021.
2. Per quanto specificamente attiene alla dottrina italiana, v. Costanzo 1996, Cassano-Contaldo 2009, Rodotà 2010, Borgia 2010, Frosini 2011, Cuocolo 2012, Bassini-Pollicino 2015.
3. Sul punto, Cerf 2012. Per Cerf la tecnologia «è un abilitatore di diritti, non un diritto in sé».
4. Negli Stati Uniti con la sentenza *Reno v. American Civil Liberties Union*, del 1997, la *Supreme Court* federale ha definito Internet come «un mezzo di comunicazione tra gli uomini di tutto il mondo unico e completamente nuovo» e, quindi, come uno strumento di esercizio della libertà di espressione; tale concetto è stato, poi, ripreso e riaffermato dalla Corte Suprema nella sentenza *Packingham v. North Carolina*, del 2017. Anche il *Conseil constitutionnel* francese, con la decisione n. 2009-580 DC del 10 giugno 2009, collegando espressamente Internet all'art. 11 della Dichiarazione del 1789, ha sottinteso che la tutela dell'accesso a Internet rappresenta un corollario della libertà d'espressione e, in quanto tale, consente lo sviluppo della personalità umana. Il *Conseil* ha, recentemente, confermato tale impostazione con la decisione n. 2020-801 del 18 giugno 2020.
5. Human Rights Council – Seventeenth session, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Frank La Rue, distribuito il 16 maggio 2011, par. 85.
6. Human Rights Council – Thirty-second session, *The promotion, protection and enjoyment of human rights on the Internet: resolution*, 18 luglio 2016, n. 1.
7. *Report of the Special Rapporteur*, cit., par. 85.

di (potenziali) utenti di Internet, caratterizzati da una situazione di particolare debolezza, e cioè le persone private della libertà, le quali, se da un lato restano titolari di diritti fondamentali[8], dall'altro vedono il loro esercizio reso sovente molto difficile. Una manifestazione di questo iato teoria/pratica si manifesta anche nella fruizione delle nuove tecnologie, al punto che non pare ozioso interrogarsi sulla compatibilità tra la possibilità di accesso a Internet e lo stato di detenzione.

Se, infatti, si promuove la premessa che un siffatto accesso costituisce una prerogativa per lo sviluppo della persona umana[9], allora esso deve essere considerato come un fattore che può concorrere a realizzare la finalità rieducativa della pena, in quegli ordinamenti che riconoscono la risocializzazione con un elemento essenziale della fase esecutiva di quest'ultima.

Segnatamente, la possibilità di utilizzare Internet negli istituti di pena può contribuire tanto a garantire l'esercizio del diritto di difesa e del diritto all'informazione[10], quanto a promuovere, sviluppare e diversificare l'offerta didattica, formativa e di lavoro per i detenuti, oltre che facilitare il mantenimento delle relazioni sociali[11].

L'accesso a Internet in istituti penitenziari può, invero, costituire la chiave per limitare il fenomeno dell'esclusione sociale causato dalla carcerazione e, dunque, in ultima analisi, per facilitare il ritorno alla vita libera, riducendo il rischio di recidiva una volta espiata la pena.

Secondo la *European Organisation of Prisons and Correctional Services*[12], nessun detenuto dovrebbe essere rilasciato senza aver acquisito alcune competenze fondamentali, tra le quali quella di utilizzare gli strumenti digitali[13]; questi ultimi

8. Secondo Rodotà «qualificare l'accesso ad Internet come diritto fondamentale è un riflesso della funzione assegnata a tale diritto come condizione necessaria per l'effettività di altri diritti fondamentali» (Rodotà 2015-a, p. 112).
9. Sul punto, si veda Reglitz 2020, pp. 314-331. Ad avviso dell'autore «Internet non è una semplice tecnologia che migliora l'efficienza, ma un mezzo per trasformare l'esistenza umana in un modo senza precedenti, che (come afferma l'ONU) "ampliando enormemente le capacità degli individui […] contribuisce al progresso dell'umanità nel suo complesso". Se ciò è corretto, allora l'accesso universale è un diritto giustificato, rendendo la mancanza di accesso una privazione ingiustificabile». Secondo Reglitz Internet, essendo di cruciale importanza per consentire la realizzazione dei diritti umani e la promozione della democrazia, deve essere libero e «fornito pubblicamente e gratuitamente a coloro che non possono permetterselo». Il libero collegamento a Internet è, infatti, «condizione necessaria per consentire l'accesso sicuro ad altri, diritti umani fondamentali incontrovertibili come la libertà di parola e la libertà di riunione», tanto che la sua mancanza costituirebbe una limitazione di tali diritti. Internet, inoltre, da un lato, – come hanno dimostrato le Primavere arabe –, «ha fornito nuovi mezzi per denunciare i crimini commessi dai governi» e, dall'altro, consente di documentare e smascherare forme di violenza ingiustificata, poiché «la possibilità per gli individui di filmare, pubblicare e condividere su Internet è molto più ampia rispetto alle tecnologie precedenti consentite, ad esempio, tramite la televisione».
10. Sul tema, si veda anche Marcelli 2011, p. 99, il quale evidenzia che Internet «ha rivelato negli ultimi anni le sue enormi potenzialità in termini di strumento di espressione, di comunicazione, di informazione e di formazione». Infatti, se si considera che «la tecnologia si presenta come un ampliamento del corpo umano», allora «secondo la visione profetica di Marshall McLuhan, Internet presenta caratteristiche tali da configurarsi come un ampliamento dell'intelletto collettivo dell'umanità».
11. Tra le regole penitenziarie europee, adottate nel 2006, la regola n. 24.1 stabilisce che «ai detenuti deve essere consentito di comunicare il più spesso possibile – tramite lettera, telefono o altre forme di comunicazione – con le loro famiglie, altre persone e rappresentanti di organizzazioni esterne, e di ricevere visite da queste persone». Inoltre, la regola n. 99 stabilisce che, a meno che non vi sia un divieto specifico per un periodo determinato da parte dell'autorità giudiziaria, i detenuti non ancora condannati, hanno accesso a libri, giornali e altri mezzi di informazione.
12. Sul punto, si veda Wilhelmsson-Jackson-Makne 2017.
13. Il progetto SPOC (*Small Private Offline Courses in Prison*), avviato nel 2018 e conclusosi nel 2021 – che ha visto coinvolte l'*Université Paul Valery* di Montpellier, la Casa Circondariale di Benevento, l'associazione Antigone Onlus e il *Centrul Pentru Promovarea Invatarii Permanente* della Romania – ha rappresentato, nell'ambiente

possono rappresentare un utile mezzo per migliorare la vita dei detenuti tanto all'interno del carcere quanto in vista del loro rilascio, ad esempio permettendo alle persone private della libertà di candidarsi a un posto di lavoro[14].

Nel rapporto anzidetto si sottolinea che, per evitare qualsiasi rischio concernente la sicurezza, è necessario un controllo delle piattaforme che permettono di accedere alla Rete, le quali, inoltre, devono essere utilizzate secondo le modalità e le tempistiche adeguate a tali esigenze.

Nelle osservazioni relative alla Raccomandazione REC(2006)2[15] del Consiglio d'Europa, è stato, altresì, ricordato che la perdita della libertà non deve ineluttabilmente esigere l'assenza di contatto con il mondo esterno e, a tal fine, «le autorità penitenziarie devono essere consapevoli delle nuove possibilità di comunicazione elettronica che la tecnologia moderna offre. Man mano che queste possibilità si sviluppano, crescono anche i modi per controllarle, cosicché le nuove modalità di comunicazione elettronica possano essere utilizzate in modi che non minaccino la sicurezza»[16].

2. I necessari limiti che si impongono alla fruizione di Internet in carcere

Laddove si voglia riconoscere che non vi sia un'incompatibilità tra il diritto – o la libertà – di accedere ad Internet e lo stato di detenzione, si deve valutare che una tale conciliabilità[17] implica, in primo

penitenziario, un elemento di innovazione pedagogica; si è trattato di un progetto volto a consentire ai detenuti la possibilità di acquisire competenze digitali, attraverso strumenti offline – e, dunque, senza utilizzare Internet –, da poter impiegare una volta al di fuori del sistema penitenziario.

14. Lo stesso Consiglio d'Europa raccomanda che le attività professionali svolte in prigione dal detenuto siano simili a quelle che, una volta fuori, possono realisticamente essere da lui esercitate.

15. Consiglio d'Europa, Comitato dei ministri, Raccomandazione REC(2006)2 del Comitato dei Ministri agli Stati membri sulle Regole penitenziarie europee, 11 gennaio 2006.

16. Consiglio d'Europa, *Règles pénitentiaires européennes*, Strasburgo, Cedex, giugno 2006, pp. 55-56. Il documento precisa che «les règles pénitentiaires européennes et les autres normes internationales en matière de droits de l'homme exigent que les prisons ne soient pas des lieux d'ennui et de monotonie» (p. 125). I detenuti, infatti, devono essere posti in grado di utilizzare il tempo trascorso in carcere in modo positivo per migliorare la propria istruzione, acquisire nuove competenze personali e professionali e prepararsi al loro rilascio. Ad avviso del Consiglio d'Europa, la maggior parte delle amministrazioni penitenziarie condivide questa prospettiva, ma la capacità di fornire un programma completo di attività per tutti i detenuti è spesso limitata. In diversi Stati membri, le persone private della libertà trascorrono ogni giorno lunghi periodi chiuse nelle loro celle o stanze, con poco da fare. Anche quando esistono opportunità di lavoro o altre attività, i compiti sono spesso di bassa qualità e di scarso valore riabilitativo, tanto che solitamente non vanno oltre la pulizia e la manutenzione domestica; inoltre, «il est de plus en plus difficile de trouver un travail approprié pour les types de plus en plus divers de détenus, y compris ceux qui souffrent de troubles mentaux ou qui abusent de drogue». In molti Stati membri, altresì, le forme tradizionali di lavoro per i detenuti non sono ritenute adatte a un mercato del lavoro in evoluzione. Il Consiglio d'Europa mette, poi, in rilievo che, sebbene la maggior parte dei sistemi carcerari cerchi di fornire una qualche forma di istruzione, spesso questa è accessibile solo ad un'esigua percentuale di detenuti. È, quindi, difficile affermare che «la prison prépare efficacement les détenus à leur retour dans la société». Tra gli esempi riportati dal Consiglio d'Europa a conferma di tali asseverazioni, vi sono la Finlandia e la Grecia; invero, in base alle «observations du CPT dans les rapports qu'il publie sur ses visites dans les Etats membres» nel 2000, in alcune carceri finlandesi, un gran numero di detenuti trascorrevano fino a 23 ore al giorno chiuso nelle loro celle, «sans guère de moyens d'occuper leur temps». Nel 2001, il Comitato ha, poi, riscontrato una situazione simile in Grecia, dove «la grande majorité des détenus qu'il a rencontrés passait l'essentiel de ses journées dans une inactivité totale» (p. 126). Quanto si dirà in seguito, mostrerà, tuttavia, come la situazione carceraria in Finlandia sia mutata nel corso del tempo, rappresentando, ad oggi, uno degli esempi più virtuosi nell'ambito dei programmi di trattamento penitenziario.

17. L'utilizzo di Internet nelle carceri, laddove permesso, ha mostrato effetti positivi sui detenuti: i contatti con il mondo esterno, infatti, sono considerati come indispensabili per contrastare gli effetti potenzialmente nocivi della condizione carceraria.

luogo, un necessario bilanciamento tra lo sviluppo della personalità umana e la sicurezza e, secondariamente, una disamina dei costi ad essa correlati.

È necessario, altresì, considerare che il tema della sicurezza pubblica si qualifica anche in relazione al reato per cui il detenuto è in carcere; infatti, vi sono alcune tipologie di illeciti penali che, in relazione alla loro gravità o alla loro natura, pongono maggiori ostacoli alla possibilità di utilizzare Internet all'interno di istituti penitenziari richiedendo dei monitoraggi e dei termini specifici[18].

La sicurezza pubblica, apprezzata nelle sue varie declinazioni, si impone, dunque, come limite negativo all'accesso ad Internet da parte dei detenuti; tale valore si collega, dal punto di vista logico-concettuale, al *quomodo* e al *quantum* atti a connotare il compimento positivo di un tale diritto o di una tale libertà.

Un'indagine, relativa tanto alle misure volte a tutelare l'incolumità pubblica quanto alla questione degli inevitabili contrappesi cui il costo di siffatto accesso è destinato a interfacciarsi, può, tuttavia, realizzarsi solo attraverso un confronto con alcune delle realtà statuali che contemplano la possibilità per le persone private della libertà di utilizzare Internet.

3. Le difficoltà in ordine all'attuazione dell'impegno da parte dello Stato di garantire l'utilizzo di Internet negli istituti penitenziari: il caso italiano

La legge del 26 luglio 1975, n. 354, rubricata "Norme sull'ordinamento penitenziario e sulla esecuzione delle misure privative e limitative della libertà", sancisce, in primo luogo, all'art. 1, comma 2, che il trattamento penitenziario «tende, anche attraverso i contatti con l'ambiente esterno, al reinserimento sociale»[19]; in secondo luogo, il terzo comma dello stesso articolo dispone che «ad ogni persona privata della libertà sono garantiti i diritti fondamentali»[20]. Tuttavia, nessuna disposizione della legge del 1975 contempla *apertis verbis* la facoltà per i detenuti di acccedere a Internet[21].

18. A mero titolo esemplificativo, meriteranno una differenziazione di trattamento – anche se sulla base di pretesti diversi –, coloro che hanno commesso reati informatici, così come i condannati per delitti inerenti all'accesso e alla diffusione di materiale pedopornografico.

19. Sul punto, Rodotà 2015. Rodotà sottolinea che «la critica alla rieducazione ha molti seri argomenti, ma soprattutto mette in evidenza come nessuna rieducazione possa essere fondata su una privazione. Il punto essenziale di questa riflessione è costituito non dall'individuazione di diritti speciali dei detenuti, ma dal riconoscimento del fatto che essi devono rimanere titolari dei diritti della persona, eccezion fatta per quelli strettamente legati alla condizione carceraria».

20. Come ha specificato anche la Corte costituzionale «l'idea che la restrizione della libertà personale possa comportare conseguenzialmente il disconoscimento delle posizioni soggettive attraverso un generalizzato assoggettamento all'organizzazione penitenziaria é estranea al vigente ordinamento costituzionale, il quale si basa sul primato della persona umana e dei suoi diritti. I diritti inviolabili dell'uomo, il riconoscimento e la garanzia dei quali l'art. 2 della Costituzione pone tra i principi fondamentali dell'ordine giuridico, trovano nella condizione di coloro i quali sono sottoposti a una restrizione della libertà personale i limiti a essa inerenti, connessi alle finalità che sono proprie di tale restrizione, ma non sono affatto annullati da tale condizione» (cfr. Corte costituzionale, n. 26, 1999, considerato in diritto, par. 3.1). In merito, si veda Ruotolo 2021, pp. 254-255. Ruotolo sottolinea come «l'applicazione di una condanna alla pena detentiva dovrebbe tradursi esclusivamente in limitazione della libertà personale, con conseguenti restrizioni della possibilità di libera locomozione. Non già in limitazione della libertà della persona, concetto senz'altro più ampio che si lega a quello di dignità e di libero sviluppo della personalità, ergendosi a precondizione per l'esercizio di tutti i diritti». Infatti, «al recluso deve essere assicurata la possibilità di esercitare tutti i diritti nei limiti della compatibilità con le esigenze di ordine e sicurezza strettamente intese».

21. Si specifica che in Italia, a partire dal 2010, sono state avanzate varie proposte di revisione costituzionale al fine di introdurre all'interno del testo fondamentale il diritto di accesso ad Internet. Inizialmente, il suggerimento di Rodotà di costituzionalizzare il diritto di accesso ad Internet, ha trovato espressione nel disegno di legge costituzionale S. 2485 del 2010, il quale si prefiggeva lo scopo di introdurre un nuovo art. 21-*bis* all'interno della Costituzione. Successivamente, i disegni di legge costituzionale S. 1317 del 2014 e C. 2769 del 2020 hanno tentato di

Pur in assenza di norme primarie penitenziarie[22] che espressamente riconoscano tale possibilità[23], l'art. 40 del "Regolamento recante norme sull'ordinamento penitenziario e sulle misure privative e limitative della libertà" (d.P.R. n. 230 del 2000), ha previsto, al primo comma, che i detenuti possono essere autorizzati dal direttore ad utilizzare, «anche nella camera di pernottamento», «personal computer», «per motivi di lavoro o di studio»; tale disposizione, però, non chiarisce se sia possibile o meno utilizzare Internet all'interno delle carceri, in quanto si limita a stabilire, al secondo comma, che «apposite prescrizioni ministeriali stabiliranno le caratteristiche, le modalità di uso e la eventuale spesa convenzionale per energia elettrica».

A tale riguardo, dunque, le circolari del DAP[24] dei primi anni 2000 hanno vietato l'utilizzo di Internet, adducendo come motivazione esigenze di sicurezza: il collegamento con l'esterno avrebbe potuto rivelarsi pregiudizievole per la salvaguardia degli istituti carcerari[25].

Tuttavia, a partire dal 2005[26], in Italia, sono state saggiate esperienze atte a includere l'utilizzo di Internet in carcere tanto con riguardo alla *formazione* professionale quanto in riferimento all'istruzione scolastica[27]. Tali pratiche hanno contribuito

inserire la modifica in esame all'interno dello stesso art. 21; in particolare la proposta del 2014 anzidetta indicava, tra i compiti della Repubblica, quello di «rimuovere gli ostacoli di ordine economico e sociale al fine di rendere effettivo questo diritto». Le proposte fin qui menzionate, erano, tuttavia accomunate dalla circostanza di disegnare il diritto di fruire della Rete come una libertà, in quanto espressione di un corollario del diritto di libera manifestazione del pensiero; il fatto, poi, che il disegno di legge S. 1317 contemplasse un obbligo prestazionale da parte dello Stato avrebbe rischiato di generare «confusione nell'originaria architettura costituzionale», in quanto tale obbligo sarebbe stato inserito «in una sede materiale tipica delle libertà negative» (cfr. Allegri 2021, p. 63). Allegri ricorda, inoltre, come la dottrina prevalente tenda «a privilegiare la qualificazione del diritto di accesso a Internet come diritto sociale a prestazione, strumentale alla realizzazione di altri diritti fondamentali, alcuni dei quali legati alla libera manifestazione del pensiero, ma molti altri attinenti piuttosto alla sfera delle libertà economiche e a quella dell'inclusione sociale e della partecipazione civica» (cfr. Allegri 2021, p. 66). Sembrano più coerenti – sebbene non privi di punti critici – con l'impostazione della dottrina maggioritaria, dunque, i disegni di legge S. 1561 del 2014 e C. 1136 del 2018, volti a introdurre in Costituzione l'art. 34-*bis*, al fine di contemplare il diritto di accesso a Internet in maniera autonoma rispetto agli altri diritti e libertà costituzionalmente garantiti; tale prospettiva pone in rilievo il fatto che Internet sia «un luogo territoriale in cui le dimensioni di spazio e tempo hanno parametri diversi rispetto al mondo fisico» (cfr. Bilancia 2011, p. 30).

22. Tuttavia, i commi 7 e 8 dell'art. 18 della legge sull'ordinamento penitenziario – così come modificati dal d.lgs. 2 ottobre 2018, n. 123 – dispongono, rispettivamente che «ogni detenuto ha diritto a una libera informazione e di esprimere le proprie opinioni, anche usando gli strumenti di comunicazione disponibili e previsti dal regolamento» e che «l'informazione è garantita per mezzo dell'accesso a quotidiani e siti informativi con le cautele previste dal regolamento».
23. Sul punto, Ruotolo 2022.
24. Dipartimento dell'Amministrazione Penitenziaria.
25. Circolare n. 3556/6006 del 15 giugno 2001 (integrata dalla circolare n. 000826 del 4 novembre 2002).
26. Sul punto, Arcangeli-Diana-di Mieri-Suriano 2010, pp. 91-99. Si veda, inoltre, Bevilacqua 2015.
27. Sul punto, Diana 2013, pp. 261 ss. Diana pone l'accento sul fatto che «l'Ordinamento Penitenziario del 1975 sottolinea (artt. 15, 17 e 19) che il trattamento del condannato e dell'internato è svolto avvalendosi principalmente dell'istruzione, del lavoro, della religione, delle attività culturali, ricreative e sportive e agevolando opportuni contatti con il mondo esterno ed i rapporti con la famiglia» (p. 268). Nel 2010, in uno studio condotto su 39.588 detenuti, era stato rilevato che «l'8,6% dei reclusi aveva un titolo di scuola superiore, il 57,2% di scuola media inferiore, il 23,1% risultava in possesso di licenza elementare e solo l'1,7 di un titolo universitario». Ad avviso dell'autore, le offerte didattiche a distanza devono tenere conto «degli effettivi bisogni formativi dei detenuti», «in considerazione anche della crescente popolazione straniera all'interno delle carceri», «altrimenti, ed il caso italiano sembra in questo senso istruttivo, l'istruzione a distanza erogata rischia di riguardare quote

a mettere in evidenza i benefici collegati all'utilizzo di Internet negli istituti carcerari.

La stessa Corte di cassazione – dovendosi esprimere in merito alla possibilità di valersi di Internet da parte di chi si trovi agli arresti domiciliari e abbia l'obbligo di non comunicare con persone diverse dai familiari e dai conviventi – ha avuto modo di chiarire che tale uso non può essere vietato *tout court* ove abbia funzione «conoscitiva o di ricerca» e, quindi, non si risolva in un mezzo per «entrare in contatto, tramite il web, con altre persone»[28].

Con la circolare del DAP del 2 novembre 2015, rubricata "Possibilità di accesso ad Internet da parte dei detenuti"[29], è stato, infine, riconosciuto che «l'utilizzo degli strumenti informatici da parte dei detenuti ristretti negli Istituti penitenziari, appare oggi un indispensabile elemento di crescita personale ed un efficace strumento di sviluppo di percorsi trattamentali complessi». Nonostante il riconosciuto valore di risocializzazione, viene sottolineato che «l'utilizzo delle moderne tecnologie informatiche nel campo del lavoro, dell'istruzione/formazione, nella gestione del servizio biblioteca interno» pone «tuttavia problemi legati alla sicurezza ed al rispetto della normativa vigente, in considerazione della particolarità del contesto detentivo». Di contro, l'esclusione di un tale utilizzo «potrebbe costituire un ulteriore elemento di marginalizzazione per i ristretti». Invero, nella circolare si sottolinea come «le Regole Penitenziarie Europee del 2006 hanno, sul punto, riaffermato il principio di un trattamento penitenziario che si avvicini il più possibile alle condizioni di vita, di organizzazione del lavoro e di studio delle persone libere»[30].

poco significative della popolazione detenuta e di non poter assolvere a pieno il suo ruolo di strumento di innovazione della formazione in carcere» (p. 266). Secondo Diana, «in una situazione come quella delle prigioni italiane, la conoscenza del detenuto in quanto persona nella sua dimensione umana sensibile e quotidiana è, però, messa in crisi dal problema del continuo sovraffollamento e dal numero estremamente basso di educatori. In questa difficoltà, l'e-learning in carcere può rappresentare un'occasione attraverso la quale è possibile non solo sviluppare innovativi strumenti didattici ma promuovere indagini di contesto per migliorare la conoscenza del detenuto».

28. Cfr. Corte di cassazione, sez. II penale, 18 ottobre 2010, n. 37151. Secondo la Cassazione «La moderna tecnologia consente oggi un agevole scambio di informazioni anche con mezzi diversi dalla parola, tramite Web, e anche tale trasmissione di informazioni deve ritenersi ricompresa nel concetto di "comunicazione", pur se non espressamente vietata dal giudice, dovendo ritenersi previsto nel generico "divieto di comunicare", il divieto non solo di parlare direttamente, ma anche di comunicare, attraverso altri strumenti, compresi quelli informatici, sia in forma verbale che scritta o con qualsiasi altra modalità che ponga in contatto l'indagato con terzi ("pizzini", gesti, comunicazioni televisive anche mediate, etc.)». Tale decisione è stata richiamata – e il suo contenuto confermato –, inoltre, da una successiva pronuncia della stessa Corte di cassazione del 2012 (Corte di cassazione, sez. IV penale, 31 gennaio 2012, n. 4064). Infine, con una decisione del 2016, la Cassazione (Corte di cassazione, sez. II penale, 8 novembre 2016, n. 46874) ha ribadito che, in caso di arresti domiciliari, «la prescrizione di non comunicare con persone estranee deve essere inteso nel senso di un divieto non solo di parlare con persone non conviventi, ma anche di stabilire contatti con altri soggetti, sia vocali che a mezzo congegni elettronici. Il messaggio diffuso sul social network, peraltro, è oggettivamente criptico per i più ed indirizzato a chi può comprendere perché sottintende qualcosa di riservato e conosciuto da una ristretta cerchia di persone ed è chiaramente intimidatorio, a dispetto del tono volutamente suggestivo, rafforzato dalle coloratissime emoticon, ancora più esplicitamente intimidatorie».

29. La circolare del 2015, in particolare, tende a «valorizzare le esperienze innovative di telelavoro, formazione e didattica a distanza, già realizzate in alcuni Istituti, dando nuova linfa al rapporto tra il carcere e il territorio in tutte le espressioni significative (imprese, scuola, università, biblioteche, enti, servizi locali etc.) che sostengono la partecipazione dei detenuti alla vita sociale e familiare».

30. In merito, Costanzo 2015, pp. 949-950. Con riferimento a quanto affermato nel preambolo della circolare del 2015, Costanzo sottolinea «una qualche propensione al riconoscimento, sia pure nell'ambito o in collegamento con i fini rieducativi, di una conformazione soggettiva dell'accesso alla Rete in cui sono trasparenti i nessi con l'art. 2 Cost., che, com'è noto mette al centro il libero svolgimento della personalità individuale anche nella

Nella circolare si legge che l'Ufficio per la Gestione del Sistema Informativo Automatizzato era già impegnato ad elaborare «un modello di riferimento omogeneo, sicuro e controllato, per tutte le strutture periferiche», al fine di «utilizzare l'infrastruttura tecnologica che sovraintende ai servizi di connettività e sicurezza in uso al Ministero della Giustizia». Alla luce di tale modello, «la configurazione delle postazioni e la predisposizione delle politiche di sicurezza saranno curate a livello centrale; mentre le limitazioni poste all'infrastruttura di rete consentiranno di instradare il singolo utente esclusivamente verso i siti (*white list*) per i quali è stato autorizzato». La circolare, altresì, prospetta «in tempi brevi», l'avviamento di «una fase di sperimentazione dell'architettura tecnica ed organizzativa».

Ai sensi dell'art. 2, comma 2, lett. c, del Protocollo d'Intesa tra il MIUR e il Ministero della Giustizia del 23 maggio 2016 – rubricato "Programma speciale per l'istruzione e la formazione negli istituti penitenziari e nei Servizi Minorili della Giustizia" –, lo Stato si è, dunque, assunto l'impegno di «avviare la progettazione, nei limiti delle risorse disponibili, di spazi formativi dotati di attrezzature tecnologiche avanzate, capaci di stabilire collegamenti virtuali tra il carcere ed il mondo esterno, con particolare riferimento agli istituti scolastici del territorio con i quali programmare e sviluppare programmi di formazione a distanza». Il contenuto di tale Protocollo è stato confermato, poi, nel 2023[31].

Ad oggi, tuttavia, non sono state ancora adempiute misure volte a realizzare gli obiettivi e le finalità che lo Stato ha prefigurato di concretizzare, a livello generale, nelle realtà carcerarie; pertanto, l'accesso a Internet rimane una prerogativa discrezionale dei singoli istituti penitenziari, con la precisazione che, laddove la navigazione sia consentita, essa deve operare sulla base delle indicazioni fornite con la circolare del 2015. Secondo tali indicazioni, i detenuti e gli internati possono accedere ad Internet solo nelle sale comuni dedicate alle attività trattamentali e la navigazione è consentita verso siti selezionati, in funzione delle esigenze legate ai percorsi trattamentali individuali, sulla base delle convenzioni/accordi stipulati con i soggetti esterni che offrono opportunità trattamentali. L'accesso ad

dimensione sociale». Tuttavia, l'autore puntualizza che tale ragionamento, «per vero, piuttosto suggestivo e avvincente nella gestione di importanti principi», «meglio si attaglierebbe alle corde del legislatore ordinario, laddove lo stesso richiamo alle Regole penitenziarie europee sembra davvero poco conferente alla specie. In tali Regole, infatti, la tensione informativa extracarceraria dei detenuti per quanto riguarda i media risulta abbastanza generica e certamente non giocata nella dimensione trattamentale, ma, com'è logico, per un documento del genere, in quello della fruizione dei diritti, peraltro con riferimento al solo detenuto imputato e non a quello condannato». Altresì, con riferimento alla «esatta base giuridica su cui la circolare in questione fonda le sue previsioni», Costanzo specifica che «scartata implicitamente (all'evidenza, sia per il silenzio assoluto sul punto, sia per il suo carattere risalente) la normativa primaria, l'unico supporto viene rinvenuto nel ridetto art. 40 della normativa di esecuzione, che in quanto consentaneo con l'utilizzo del personal computer, è assunto come espressivo di una ratio più generale intesa a favorire ogni altra applicazione del mezzo per incrementare le opportunità rieducativa». Malgrado ciò, tale ricostruzione appare all'autore «abbastanza fragile dato che il richiamo al trattamento rischia di provare troppo, aprendo la strada a qualsiasi altra sperimentazione basata sulla mera previsione circolare, mentre il riferimento al mezzo difficilmente sarebbe suscettibile di un'interpretazione estensiva data la minuziosità anche tecnica del precetto regolamentare di cui al precipitato art. 40».

31. L'art. 1, comma 4, lett. d, del Protocollo di intesa del 2023, dedicato alla «Prosecuzione del programma speciale per l'istruzione e la formazione negli istituti penitenziari e nei servizi minorili della giustizia», prevede «la valorizzazione delle tecnologie dell'informazione e della comunicazione, sia per la realizzazione di percorsi di fruizione a distanza (FAD), sia al fine di colmare il divario digitale dei soggetti in esecuzione pena detentiva e non detentiva, in considerazione del fatto che la conoscenza in campo digitale è ormai indispensabile per ogni tipo di attività lavorativa, di istruzione/formazione, economica ed associativo/relazionale, con conseguente permanere di un significativo svantaggio sociale per chi non ha i mezzi o le possibilità per accedervi». L'art. 1, comma 5, lett. n, del Protocollo in esame prevede, inoltre, il «potenziamento delle infrastrutture tecnologiche utilizzate per i colloqui e per le attività di formazione e allestimento delle aree specificamente predisposte per l'utilizzo dei *device*».

Internet, altresì, è consentito di regola nei circuiti a custodia attenuata e media sicurezza, mentre «per i detenuti appartenenti al circuito alta sicurezza o sottoposti a regimi particolari, le direzioni devono considerare caso per caso le particolari ragioni ed i benefici attesi secondo il progetto d'Istituto ed il programma di trattamento individualizzato, dandone comunicazione al competente Ufficio III della Direzione Generale Detenuti e Trattamento per eventuali osservazioni». Non è, in nessun caso, consentito l'accesso ad Internet ai detenuti sottoposti al regime ex art. 41-*bis* della legge sull'ordinamento penitenziario.

All'interno della circolare del 2015, inoltre, si specifica che, poiché – conformemente al quadro normativo europeo – «il disegno di legge governativo n. 2798 […] prevede […] di sostenere il diritto all'affettività in carcere e di favorire le relazioni familiari, anche utilizzando i collegamenti audiovisivi», «con nota del Vice Capo Vicario n. 0034193 del 29/01/2014» era stato richiesto «alle Direzioni degli istituti di fornire notizie in merito ad eventuale avvio del sistema di comunicazione via *Skype*», ove le dotazioni informatiche lo consentissero». Non essendo «emerse criticità in merito all'utilizzo di tale strumento» […] «tutte le strutture ove sono allocali detenuti comuni» erano state invitate «ad implementare l'utilizzo di tale strumento o, ove ritenuto di maggiore garanzia per le esigenze di sicurezza, la piattaforma *Microsoft Lync*».

In linea con la circolare anzidetta, il documento finale degli Stati Generali dell'esecuzione penale (da ultimo aggiornato il 18 aprile 2016)[32], al punto 3.4.1 ("Colloqui, corrispondenza elettronica e collegamenti audiovisivi"), ha proposto di integrare l'art. 18 della legge sull'ordinamento penitenziario «mediante l'inserimento di un comma mirante a consentire l'utilizzo di programmi di conversazione visiva, sonora e di messaggistica istantanea che presuppongono l'accesso – ovviamente con gli opportuni controlli – alla rete internet». Altresì, il documento ha suggerito «di equiparare alla corrispondenza telefonica l'accesso al collegamento audiovisivo con tecnologia digitale, con la prospettiva che nel prossimo futuro i due tipi di collegamento (telefonico e via rete internet) potranno essere indifferentemente utilizzati dai detenuti»[33].

La legge delega n. 103 del 2017, quindi, ha compreso, tra i principi e criteri direttivi che i decreti legislativi recanti modifiche all'ordinamento giudiziario erano tenuti a rispettare[34], la «disciplina dell'utilizzo dei collegamenti audiovisivi sia a fini processuali, con modalità che garantiscano il rispetto del diritto di difesa, sia per favorire le relazioni familiari» (art. 1, comma 85, lett. i). Nella Relazione illustrativa dello schema di decreto legislativo[35] si leggeva, poi, che «allo scopo di favorire le relazioni familiari ed affettive (criterio i) della delega sulla disciplina dell'utilizzo dei collegamenti audiovisivi non solo a fini processuali ma anche per favorire le relazioni familiari, si è ritenuto opportuno consentire l'uso delle tecnologie informatiche all'interno del carcere, anche per i contatti con la famiglia (ad esempio, attraverso l'uso della posta elettronica e dei colloqui via *Skype* che consentono, altresì, la trasmissione di messaggi istantanei)». Pertanto, con riferimento all'art. 18 della legge sull'ordinamento penitenziario, si prevedeva di aggiungere «un nuovo comma, inserito subito dopo quello che disciplina le conversazioni telefoniche (rimasto inalterato)», deputato a disporre «che detti colloqui possano avvenire anche mediante programmi di conversazione visiva, sonora e di messaggistica istantanea, attraverso la connessione internet (ad esempio, attraverso *Skype*), essendo in tali casi da equipararsi a tutti gli effetti a quelli telefonici[36]». Nella Relazione in esame si dava, altresì, atto che

32. Il documento in esame è consultabile sul sito del Ministero della Giustizia.

33. In merito, Locchi-Pettinari 2020, p. 28.

34. Infatti, l'art. 1, comma 82, della legge delega in esame prevedeva che il Governo era delegato «ad adottare decreti legislativi […] per la riforma dell'ordinamento penitenziario, secondo i principi e criteri direttivi previsti dai commi 84 e 85».

35. V. il testo della Relazione.

36. Tuttavia, nella Relazione si esclude che «la facoltà di utilizzare tali strumenti informatici possa essere estesa anche ai detenuti e internati per i reati indicati nell'articolo 41-*bis* ord. pen. La limitazione si è resa necessaria in considerazione delle necessarie cautele da approntare, per ragioni di sicurezza, nei confronti di tale categoria di

«attualmente solo 17 istituti penitenziari sono dotati di *Skype* per i colloqui».

Tuttavia, i decreti legislativi n. 121, 123, 124 del 2 ottobre 2018, pubblicati in *Gazzetta Ufficiale* il 26 ottobre 2018, che hanno concluso la riforma sull'ordinamento penitenziario, non hanno introdotto modifiche volte a disciplinare quanto disposto dall'art. 1, comma 85, lett. i, della legge delega del 2017.

Solo con la lettera circolare del DPA del 29 gennaio 2019, avente l'obiettivo di facilitare le relazioni familiari nelle strutture penitenziarie, sono state fornite «le indicazioni per agevolare le attività e predisporre gli interventi necessari a rendere fruibile – su vasta scala – l'utilizzo della piattaforma *Skype for business* (ex *Microsoft Lync*) per l'effettuazione di videochiamate[37] da parte dei detenuti ed internati appartenenti – in questa prima fase di avvio – al circuito media sicurezza con i familiari e/o conviventi».

Con una pronuncia del 2019, la Corte di cassazione[38] ha, quindi, ricordato che la materia dei colloqui a distanza non è disciplinata dalla legge «né per i detenuti in regime ordinario, né per detenuti sottoposti al regime di cui all'art. 41-*bis* ord. pen.». Ad avviso della Cassazione, infatti, è opportuno che sia «la legge o un regolamento a disciplinare la materia, stabilendo in che misura i colloqui telefonici consentiti dalle norme richiamate possano essere estesi a quelli videotelefonici, ovvero se i colloqui telefonici possano essere sostituiti da forme diverse di comunicazione a distanza anche visiva rese possibili dal progresso tecnologico, stabilendo, quindi, gli strumenti e le attrezzature da adottare, le regole (più o meno restrittive con riferimento al regime cui sono sottoposti i detenuti), le voci di spesa, i poteri delle Direzioni dei penitenziari e del personale di polizia penitenziaria». Secondo la Corte l'intervento del legislatore non è destinato ad esaurirsi in una esigenza meramente formale tesa al «rispetto doveroso della legge reso, se possibile, ancora più stringente con riferimento ai detenuti sottoposti al regime di cui all'art. 41-*bis* ord. pen.», ma è volto ad esprimere il principio «di parità di trattamento tra i detenuti, che rischia di essere severamente violata affidando ai singoli Magistrati di Sorveglianza la verifica della praticabilità in concreto delle soluzioni tecnologiche ipotizzate».

La Cassazione, nel 2021[39], si è, poi, espressa sulla ragionevolezza della preclusione di utilizzare il sistema *Skype* da parte dei detenuti sottoposti al regime di cui all'art. 41-*bis*; nel caso di specie, tuttavia, tale aspetto è stato valutato, non in merito alla necessità di favorire le relazioni familiari ed affettive, ma in relazione al diritto allo studio[40]. La Corte, nello specifico, ha ricordato non solo che l'utilizzo di *Skype* per il sostegno scolastico non è previsto dalla normativa penitenziaria, ma anche che «il diritto allo studio del detenuto, garantito da norme di legge nazionali e sovranazionali, d[eve] essere necessariamente contemperato con le esigenze di ordine e di sicurezza sottese al regime differenziato ex art. 41-*bis* ord. pen., con la conseguenza che non [è] individuabile alcuna lesione grave ed attuale del diritto allo studio e alla formazione, laddove questo [è] garantito e assicurato […] seppure con alcune limitazioni rese indispensabili dall'interesse pubblico al mantenimento della sicurezza».

Successivamente, nella relazione finale[41] della Commissione per l'innovazione del sistema

detenuti ed internati e, in particolare, tenuto conto del peculiare regime previsto dall'articolo 39, comma 7, d.P.R. 30 giugno 2000, n. 230 in tema di corrispondenza telefonica. La citata disposizione prevede, infatti, che delle conversazioni telefoniche autorizzate su richiesta degli stessi ne sia sempre disposta la registrazione».

37. La circolare del 2019 specifica «che, ai fini dell'inquadramento giuridico della fattispecie e del richiamo all'apparato normativo di riferimento, la videochiamata è da equipararsi ai colloqui».
38. Corte di cassazione, sez. I penale, 22 marzo-16 aprile 2019, n. 16577.
39. Corte di cassazione, sez. VII penale, 31 marzo 2021, n. 12199.
40. L'art. 14.1 della circolare del DAP n. 367/6126 del 2 ottobre 2017, contente le disposizioni relative alla organizzazione del circuito detentivo speciale previsto dall'art. 41-*bis* della l. 26 luglio 1975, n. 354 (ordinamento penitenziario), dispone che il detenuto, qualora frequenti corsi scolastici o universitari cui è regolarmente iscritto e rispetto ai quali si rende indispensabile l'uso di strumenti e supporti informatici, può fruire, previa richiesta, di computer fissi o di apparecchi privi di «connessioni esterne (wi-fi, bluetooth, connessione dati)».
41. La relazione finale, del 17 dicembre 2021, è consultabile sul sito del Ministero della Giustizia.

penitenziario (istituita con il decreto ministeriale del 13 settembre 2021), sono state «elaborate alcune proposte di azioni amministrative»; in particolare, l'azione 4, dedicata alla didattica a distanza, ha ricordato che «l'esperienza "COVID-19[42]" ha dimostrato» che tale tipologia di didattica – che deve, però, affiancarsi a quella in presenza – può «avvenire in sicurezza»[43,44].

Inoltre, l'azione 7, relativa alla questione della disponibilità dei computer, propone di «incentivare il possesso di computer nelle stanze di pernottamento, secondo quanto proposto con la revisione dell'art. 40 del regolamento di esecuzione. Mediante circolare si potrebbe specificare la destinazione di appositi locali per l'impiego di personal computer con connessione ad Internet attraverso una piattaforma protetta e dedicata del Ministero della Giustizia, la quale filtri e impedisca l'accesso ai contenuti non consentiti».

Invero, la Commissione soprammenzionata propone di modificare l'art. 40 del DPR. n. 230/2000, prevedendo che «salvo inderogabili esigenze attinenti alla prevenzione dei reati, ovvero per ragioni di sicurezza, è autorizzato l'uso personale, anche nella camera di pernottamento, di dispositivi elettronici per attività di svago, di studio o di lavoro, con esclusione della possibilità di connessione internet, connessione cellulare o altro tipo di connessione a corto o lungo raggio». La Commissione, a sostegno della riforma suggerita, ha sottolineato che «la proposta, rispondendo ad un'esigenza fatta propria dalla Regole penitenziarie europee, mira ad informare la quotidianità penitenziaria alla vita libera, consentendo alla persona detenuta di accedere agli strumenti tecnologici per le stesse ragioni per le quali se ne fruisce all'esterno, con l'unico limite dell'accesso ad Internet, connesso ad evidenti esigenze di sicurezza. Si intende dunque rimodernare il testo attuale, che fa ancora riferimento a strumenti tecnologici desueti, consentendo l'accesso pacifico ai lettori cd e dvd, o agli e-reader, per ragioni anche di mero svago, e consentendo in modo ampio l'uso del personal computer, di cui si dovrà curare la possibilità anche di acquisto al sopravvitto»[45].

42. Sul punto, Mollo 2022, pp. 64-65. Mollo puntualizza che «durante l'emergenza provocata dal coronavirus, infatti, la didattica a distanza (Dad) svolta nelle carceri in forza della circolare del 2019 sopra richiamata ha subito una brusca sospensione nei primi mesi, per poi stentare a diffondersi uniformemente nel tempo perché soltanto pochi detenuti hanno potuto disporre dell'accesso a Internet attraverso videochiamate e lezioni *in streaming*».
43. In ordine all'esigenza di sicurezza, si veda Baratta 2001, p. 22 ss. Secondo l'autore, per realizzare una «politica integrale di protezione e soddisfazione dei diritti umani e fondamentali», il «diritto alla sicurezza» dovrebbe essere sostituito dalla «sicurezza dei diritti». In linea con la prospettiva di Baratta, che disegna il diritto alla sicurezza come un elemento accessorio, si veda Ruotolo 2022, p. 10. Ruotolo, infatti, precisa che «in una teoria dei diritti costruita opportunamente come teoria dei bisogni, che cioè concepisca i diritti come proiezione normativa dei bisogni, non pare contestabile la secondarietà del diritto alla sicurezza rispetto agli altri bisogni c.d. basici o reali».
44. Nella relazione si legge, inoltre, che «i Corsi scolastici ad oggi vengono attivati, tramite piattaforma, dal personale che apre il collegamento e rimuove la strumentazione (mouse e tastiera). L'interazione dei detenuti con i docenti avviene attraverso il monitor. La vigilanza e il controllo sono assicurate secondo l'organizzazione propria di ciascun istituto (in presenza o a distanza). Meritano attenzione i lavori dipartimentali (DGMC) volti alla creazione di piattaforme e-learning, con metodologie di apprendimento e formazione, alternative all'insegnamento in aula, che si sviluppano su una rete interna adeguatamente configurata e chiusa (senza possibilità di accedere ad Internet) e che consentono, con una gestione multilingue, di distribuire materiali e corsi in modo aggiornato, con spazi di interattività e collaborazione. Le modalità di utilizzo di questo strumento sono l'apprendimento in forma autonoma in autoformazione e/o quello parzialmente assistito con tutoraggio, diverso da quello basato sull'interazione con l'insegnante (piattaforma *moodle* che utilizza forum, chat o verifiche come quiz). Ovviamente sono previste giornate con possibilità di incontri in presenza. Bisognerebbe poi (ai sensi dell'art. 42 R.E.) incentivare la possibilità di continuare la formazione dopo la dimissione dall'istituto anche per le persone in misura alternativa. In questa direzione si segnala la presenza di scuole che mettono a disposizione locali dove gli affidati possano collegarsi per continuare i percorsi formativi» (pp. 202-203).
45. Si vedano, in particolare, le pp. 59-60 della relazione in esame.

Tuttavia, anche la proposta da ora delineata non ha trovato, al momento, una sua realizzazione, mettendo in luce che «la difficoltà con cui anche quelle che appaiono riforme di mero buon senso e di civiltà giuridica stentano ad affermarsi rende manifesto, ancora una volta, come il carcere rappresenti non solo un tema complesso e diviso sul piano politico e sociale, ma risulti anche caratterizzato da un grave immobilismo interno»[46].

Quanto si è venuti dicendo dimostra che l'attuazione dei «buoni propositi» sia ormai improrogabile, non solo per concretizzare il principio personalista in riferimento a soggetti particolarmente deboli quali i detenuti[47], ma anche per dare un senso alla finalità rieducativa della pena.

4. La Corte europea dei diritti dell'uomo e il mancato riconoscimento di un obbligo generale di garantire ai detenuti l'accesso a Internet

Viste le difficoltà di creare le condizioni per una reale fruizione di Internet all'interno degli istituti penitenziari italiani, ci si può chiedere se, nel tessuto ordinamentale europeo, esista davvero un diritto a Internet dei detenuti.

Sul punto, la Corte europea dei diritti dell'uomo ha fatto aperture solo limitate, esprimendosi in merito ai limiti cui può essere subordinato l'accesso a Internet, alle finalità che, generalmente, giustificano l'utilizzo di Internet in carcere e, conseguentemente, alla qualità dei siti e dei contenuti di cui il detenuto può beneficiare. Tuttavia, la Corte EDU, nelle sue pronunce, non ha individuato alcuna norma idonea a edificare l'accesso a Internet, in istituti di pena, come un diritto sociale.

In primo luogo, in Lituania, nel 2006, un detenuto, laureato in medicina, della Casa di Correzione Pravieniškės, si era visto rifiutare la richiesta di accedere al sito AIKOS, gestito dal Ministero dell'Istruzione e della Scienza, al fine di seguire i corsi universitari per ottenere una seconda laurea. La motivazione del rifiuto della direzione del carcere si reggeva sull'affermazione che concedere ai detenuti di utilizzare la Rete avrebbe significato permettere loro di continuare le proprie attività criminali. Inoltre, sebbene l'articolo 96[48] del Codice dell'esecuzione delle sentenze (*Bausmių vykdymo kodeksas*)[49] accordasse alle persone private della libertà di utilizzare il computer, da ciò, secondo le autorità penitenziarie, non poteva dedursi il diritto di usare Internet.

La Corte EDU, alla quale il signor Jankovskis aveva fatto ricorso, nella propria decisione, del 2017[50], ha sottolineato che, trattandosi di un sito gestito dal Ministero dell'Istruzione e della Scienza, l'accesso ad esso da parte di un detenuto non

46. Cfr. Menghini 2022, p. 423.
47. Pur in assenza di una costituzionalizzazione del diritto di accesso ad Internet in Italia, si deve considerare che «se è vero che Internet costituisce ormai a pieno titolo uno strumento di esercizio dei diritti di cittadinanza e di sviluppo della persona, e che l'impossibilità di accedervi comporta rischi di esclusione sociale direttamente incidenti sul livello di eguaglianza sostanziale, allora non sembra contestabile che il fondamento costituzionale del diritto di accesso debba oggi ravvisarsi negli artt. 1, 2, 3 Cost.» (cfr. Valastro 2011, p. 47). Infatti, «nella ricerca di un ancoraggio costituzionale ad Internet, l'art. 2 non può […] essere di per sé sufficiente», in quanto il «richiamo congiunto all'art. 3, comma 2, è troppo forte per poter essere collocato in secondo piano. Le due disposizioni formano, in effetti, un sistema di per sé inscindibile, giacché la dimensione virtuale di svolgimento della personalità non potrebbe in alcun caso sussistere se non ci fosse, a monte, l'opera di rimozione degli ostacoli da parte della Repubblica» (cfr. Passaglia 2014, p. 19).
48. Tale articolo dispone che i detenuti, possono utilizzare televisori, computer, lettori video e audio, radio, playstation e altri oggetti indicati nel Regolamento interno delle carceri; queste apparecchiature devono essere acquistate servendosi di denaro depositato nei conti personali dei detenuti o loro consegnato dal coniuge, partner o parente stretto. Inoltre, l'articolo in esame specifica che le norme che disciplinano l'uso di tali strumenti sono stabilite nel Regolamento interno delle singole strutture penitenziarie.
49. L'articolo 10 del Codice dell'esecuzione delle sentenze puntualizza che i condannati godono di tutti i diritti, le libertà e i doveri stabiliti dalla legge per i cittadini lituani con le restrizioni stabilite dalla legge o dalla sentenza del tribunale.
50. Corte europea dei diritti dell'uomo, *Jankovskis c. Lituania*, 17 gennaio 2017, ric. 21575/08.

avrebbe rappresentato un rischio per la sicurezza del carcere. Inoltre, la Corte ha puntualizzato[51] che le autorità lituane non si erano soffermate ad esaminare l'argomentazione del ricorrente secondo cui l'accesso a un determinato sito web era necessario per la sua istruzione. Invero, anche se «le autorità dell'istituto penitenziario di Pravieniškės hanno sottolineato la presenza di una scuola secondaria in tale carcere, nonché la possibilità di seguire corsi di informatica presso la scuola professionale *Elektrėnai*», tuttavia, questa era sembrata «una proposta molto distante rispetto al desiderio del richiedente di acquisire un secondo titolo universitario». Inoltre, la Corte ha precisato che le autorità penitenziarie o i tribunali lituani non hanno cercato di sostenere il rifiuto sulla base del fatto che un accesso esteso a Internet avrebbe potuto comportare costi aggiuntivi per lo Stato. Ciò è risultato ancora più rilevante, allorché la Corte ha ricordato che l'accesso a Internet «è sempre più inteso come un diritto, e sono state avanzate richieste per sviluppare politiche efficaci per raggiungere l'accesso universale a Internet e superare il divario digitale»[52]. Malgrado tali affermazioni, la Corte EDU non ha individuato norme volte a porre in capo agli Stati l'obbligo di garantire la fruizione di Internet alle persone private della libertà; essa, infatti, si è limitata a ravvisare, nel caso in esame, la violazione dell'articolo 10 della Convenzione europea dei diritti dell'uomo (CEDU), relativo alla libertà di pensiero, coscienza e religione, sul presupposto che «l'ingerenza nel diritto del ricorrente a ricevere informazioni, nelle circostanze specifiche del caso di specie, non può essere considerata necessaria in una società democratica[53]».

La Corte di Strasburgo si era già occupata nel 2016 del tema relativo all'accesso a Internet da parte dei detenuti e, anche in tale occasione, aveva affermato che disconoscere tale diritto, in presenza di precise condizioni, implica violare l'articolo 10 CEDU[54]. Nella situazione specifica, era stato negato a un detenuto, condannato all'ergastolo in Estonia, la possibilità di accedere a tre siti Internet per consultare la versione online della Gazzetta dello Stato, le decisioni della Corte Suprema e dei tribunali amministrativi e, infine, il database HUDOC delle sentenze della Corte europea dei diritti umani.

La Corte, nella propria decisione, aveva precisato che l'articolo 10 della Convenzione anzidetta non può essere interpretato nel senso che esso imponga un obbligo generale di garantire ai detenuti l'accesso a Internet (o a siti Internet specifici); tuttavia, nel caso di specie, la Corte aveva ritenuto che il diniego di consultare tali pagine web costituiva un'ingerenza – arbitraria – nel diritto a ricevere informazioni, poiché la legge estone (*Imprisonment Act*) consente l'accesso a – determinati – siti contenenti informazioni giuridiche. Infatti, la Corte aveva sottolineato che ai sensi dell'*Imprisonment Act*, ai detenuti è concesso un accesso limitato a Internet tramite computer appositamente adattati a tale scopo e sotto il controllo delle autorità penitenziarie; pertanto, «sono state comunque adottate le misure necessarie per l'utilizzo di Internet da parte dei detenuti e i relativi costi sono stati sostenuti dalle autorità[55]». Ad avviso della Corte, «i tribunali nazionali non hanno intrapreso un'analisi dettagliata dei rischi per la sicurezza che emergerebbero dall'accesso ai tre ulteriori siti web in questione, anche tenendo conto del fatto che si trattava di siti web di autorità statali e di un'organizzazione internazionale»; invero, come ricordato nella decisione, la Corte Suprema estone aveva motivato il proprio giudizio sulla base dell'asserzione che accordare l'accesso a ulteriori indirizzi web avrebbe potuto aumentare il rischio che i detenuti intraprendessero comunicazioni vietate, fondando, così, l'esigenza di maggiori livelli di monitoraggio. Tuttavia, né la Corte Suprema né il Governo estoni, ad avviso della Corte di Strasburgo, erano riusciti a dimostrare in modo convincente che elargire al ricorrente la consultazione dei tre siti summenzionati avrebbe causato costi aggiuntivi degni di nota; pertanto, nella decisione era stata sottolineata la mancata deduzione di ragioni sufficienti a

51. *Ivi*, par. 61.

52. *Ivi*, par. 62.

53. *Ivi*, par. 64.

54. Corte europea dei diritti dell'uomo, *Kalda c. Estonia*, 19 gennaio 2016, ric. 17429/2010.

55. *Ivi*, par. 53.

giustificare l'ingerenza dello Stato nel diritto del ricorrente a ricevere informazioni.

In conclusione, la Corte europea dei diritti dell'uomo è tornata a pronunciarsi sulla questione nel 2021[56]; il ricorrente, «facendo riferimento alle sentenze Kalda […] e Jankovskis […] resa dalla Corte», aveva sostenuto «che il rifiuto delle autorità penitenziarie di autorizzarlo ad accedere ai siti web della Corte, della Corte Costituzionale e della Gazzetta Ufficiale costituis[se] un'ingerenza nell'esercizio del suo diritto a ricevere informazioni o idee compreso nel suo diritto alla libertà di espressione garantito dall'articolo 10 della Convenzione»[57]. Autorizzando la legge turca l'accesso dei detenuti a Internet per fini educativi e di reinserimento – ai sensi dell'art. 90, commi 3 e 4, del Regolamento relativo alla gestione degli istituti penitenziari e all'esecuzione delle pene e delle misure di prevenzione – il ricorrente aveva, in primo luogo, precisato che la sua richiesta era finalizzata alla preparazione della propria linea difensiva e, quindi, essenziale per l'esercizio dei suoi diritti di difesa; in secondo luogo Ramazan Demir, essendo un avvocato di professione, aveva sottolineato che la sua istanza «di accesso ai siti web della Corte, della Corte Costituzionale e della Gazzetta Ufficiale per informarsi sulle recenti sentenze e decisioni di queste due giurisdizioni […] gli avrebbe permesso di continuare il suo sviluppo personale e professionale[58]». Ad avviso del richiedente, altresì, «il diritto di accesso a Internet di un detenuto è garantito in due situazioni: o tale diritto è riconosciuto dal diritto interno, oppure l'accesso a Internet è necessario per l'esercizio di altri diritti riconosciuti dal diritto interno».

In linea con quanto da ultimo riportato, tra i terzi interventori, l'associazione *İfade Özgürlüğü Derneği* ha sostenuto che, «anche se un diritto generale dei detenuti ad accedere a Internet non discende dal diritto a ricevere informazioni o idee, tutelato dall'articolo 10 della Convenzione, esso deriva dai principi stabiliti dalla Corte nelle decisioni Kalda e Jankovskis sopra citate secondo cui i detenuti possono avere il diritto di accesso a Internet nei casi in cui tale diritto è riconosciuto dal diritto interno o se tale accesso è necessario per l'esercizio di un diritto riconosciuto dal diritto interno». Ad avviso dell'associazione anzidetta, «tenendo conto dello sviluppo di Internet come mezzo di diffusione delle informazioni nel mondo di oggi e del principio di normalizzazione delle condizioni di vita carceraria, i detenuti devono beneficiare di un accesso più ampio a Internet al fine di garantire l'esercizio dei loro diritti fondamentali[59]».

La Corte, nel caso di specie, si è, ancora una volta, limitata a puntualizzare che, «poiché l'accesso dei detenuti a determinati siti Internet a fini di formazione e reinserimento era già previsto dalla legge turca, la restrizione dell'accesso del ricorrente ai siti Internet della Corte, della Corte Costituzionale e della Gazzetta Ufficiale, che contengono soltanto informazioni giuridiche atte a servire allo sviluppo e alla riabilitazione dell'interessato nell'ambito della sua professione e dei suoi centri di interesse, costituisce un'ingerenza nell'esercizio del diritto del richiedente a ricevere informazioni»[60]. Ad avviso della Corte di Strasburgo, infatti, «i giudici nazionali non hanno effettuato un'analisi dettagliata dei rischi per la sicurezza che sarebbero derivati dall'accesso del ricorrente ai tre siti web summenzionati, soprattutto perché si trattava di siti web di autorità statali e di un'organizzazione internazionale e che il ricorrente ha avuto accesso solo a questi siti web sotto il controllo delle autorità e alle condizioni che queste ultime avrebbero determinato».

Alla luce delle pronunce esaminate, dunque, la Corte EDU, ad oggi, non riconosce in capo agli Stati un obbligo generale di assicurare l'accesso ad Internet all'interno degli istituti penitenziari.

5. Profili di diritto comparato

La giurisprudenza della Corte di Strasburgo, nel suo evitare di prendere esplicitamente e risolutamente posizione in favore del diritto a Internet delle persone private della libertà personale, lascia,

56. Corte europea dei diritti dell'uomo, *Ramazan Demir c. Turchia*, 9 febbraio 2021, ric. 68550/2017.
57. *Ivi*, par. 19.
58. *Ivi*, par. 21.
59. *Ivi*, par. 27.
60. *Ivi*, par. 38.

inevitabilmente, un ampio margine di apprezzamento in favore degli Stati. Tale discrezionalità è talmente ampia che, persino quando di diritto può parlarsi, la configurazione dell'accesso a Internet dei detenuti può avere una struttura profondamente diversa. A tal riguardo, è necessario premettere, infatti, che – laddove non vietato – vi sono Stati che elevano l'accesso a Internet, da parte dei detenuti, a un diritto sociale e altri che lo declinano come una libertà.

Al fine di richiamare l'attenzione sui diversi profili che emergono da una siffatta classificazione si prenderanno in esame, tra gli Stati che configurano l'accesso a Internet come un diritto sociale, la Finlandia e la Norvegia e, tra gli ordinamenti che circoscrivono l'utilizzo della Rete a una mera libertà, la Spagna, la Francia e il Belgio. Se, infatti, queste ultime realtà statuali prevedono la possibilità per i detenuti di utilizzare Internet, lo Stato, ad oggi, non assume l'obbligo di assicurare questo vantaggio in tutti gli istituti carcerari, anche in ragione dei costi ad esso correlati.

L'indagine che segue è volta ad esaminare le soluzioni offerte dai Paesi summenzionati, per comprendere se esse rivelino problematiche affini a quelle evidenziate nell'approfondimento dell'esperienza italiana o, di contro, possano offrire suggestioni idonee a dirimere le criticità osservate in quest'ultima.

5.1. L'accesso a Internet da parte dei detenuti quale libertà: i casi del Belgio, della Spagna e della Francia

Il Belgio, la Spagna e la Francia – seppure con le proprie peculiarità – possono essere ricondotti nell'alveo degli ordinamenti che declinano l'accesso a Internet in istituti penitenziari come una libertà.

In Belgio, la legge del 12 gennaio 2005 – rubricata "*Loi de principes concernant l'administration des établissements pénitentiaires ainsi que le statut juridique des détenus*" – dispone, all'art. 65, comma 1, che «è vietato qualsiasi mezzo di telecomunicazione tra un detenuto e l'esterno del carcere che non sia autorizzato da o ai sensi di questa legge»[61]. Tuttavia, il secondo comma dell'articolo anzidetto precisa che «il Re, per scopi di formazione, può prevedere l'accesso da parte dei detenuti a mezzi di telecomunicazione diversi da quelli autorizzati dalla presente legge». In particolare, all'art. 4, comma 3, dell'*arrêté royal* del 26 giugno 2019, si prevede che il detenuto può seguire attività di formazione anche a distanza; tuttavia, non vi sono norme idonee ad accordare, in capo allo Stato, alcun obbligo generale di garantire l'accesso a Internet[62], la facoltà di fruire della quale si declina, dunque, come una mera libertà.

Il carcere belga di Beveren, dal 2014, rappresenta uno dei primi esempi di prigioni tecnologiche: ciascuna cella è stata dotata di un computer, che permette di accedere ad alcuni servizi online attraverso la piattaforma *Prison cloud*. Quest'ultima è stata messa a disposizione di tre penitenziari di nuova edificazione[63], i quali, al momento, rappresentano gli unici istituti carcerari del Belgio idonei a garantire alle persone private della libertà la possibilità di accedere a Internet.

Attraverso la piattaforma *Prison cloud*, inserendo il proprio identificativo, i detenuti possono chiedere la copia del loro fascicolo giudiziario, ma allo stesso tempo fruire di corsi da remoto, possono prenotare libri della biblioteca e svolgere videochiamate; queste ultime non possono essere ascoltate – salvo autorizzazione del giudice – dall'amministrazione penitenziaria, la quale, pertanto, deve limitarsi a sorvegliare la lista dei numeri contattati dai detenuti.

Inoltre, le persone private della libertà hanno il diritto di consultare alcuni indirizzi web, preselezionati in modo tale da eludere il rischio che essi possano comunicare con l'esterno senza l'adeguato controllo delle autorità competenti. A tale ultimo riguardo, bisogna, però, precisare che nel mese del settembre 2014, alcuni detenuti erano riusciti,

61. La sezione IV, rubricata "*de l'usage du téléphone et autres moyens de télécommunication*", del capitolo III – dedicato ai contatti con il mondo esterno – della legge del 2005, omette di individuare in maniera espressa i mezzi di telecomunicazione il cui uso è ammesso.
62. Nell'*arrêté royal*, ad esempio, si prevede che la piattaforma online sia messa a disposizione dal "*dispensateur de la formation*".
63. Si tratta delle prigioni di Beveren, di Marche-en-Famenne e di Leuze-en-Hainaut.

attraverso una funzione del sito del VDAB[64], ad inviare e-mail, delle quali si erano serviti per continuare a svolgere alcune attività criminali. Tale vicenda, sebbene risolta, ha mostrato la necessità di una costante vigilanza.

Il *Reglamento Penitenciario* spagnolo, così come modificato nel 2022 (decreto reale n. 268/2022), prevede, all'art. 4, comma 3, che i diritti menzionati dal comma 2 dell'articolo in esame – come il diritto alle relazioni, il diritto al lavoro retribuito, il diritto di presentare istanze e denunce alle autorità penitenziarie e giudiziarie, al Difensore civico e alla Procura della Repubblica, nonché di rivolgersi alle autorità competenti e di avvalersi dei mezzi di difesa dei propri diritti e interessi legittimi – e altri «*que puedan derivarse de la normativa penitenciaria*» possono essere esercitati attraverso le tecnologie dell'informazione e della comunicazione, subordinatamente, però, alle possibilità materiali e tecniche di ciascun centro penitenziario. Ad ogni modo, nell'esercizio di tali diritti devono essere sempre rispettati i principi in materia di sicurezza digitale e protezione dei dati, così come le norme relative al regolamento interno del carcere.

Con riguardo al diritto per i detenuti di comunicare con i familiari, i propri amici o i propri rappresentanti legali, l'art. 41, dopo aver delineato le tipologie di comunicazioni di cui il detenuto può beneficiare, al comma 8, in seguito alle modifiche intervenute nel 2022, prevede che tali comunicazioni possono essere effettuate – nel rispetto dei principi vigenti in materia di sicurezza digitale e protezione dei dati[65] – mediante l'uso di tecnologie dell'informazione e della comunicazione e di sistemi di videoconferenza, a seconda delle possibilità materiali e tecniche di ciascun istituto penitenziario.

Inoltre, ai sensi del nuovo art. 127, comma 4, a seconda delle possibilità materiali e tecniche di ciascun centro penitenziario, le biblioteche possono disporre di punti di accesso alle reti di informazione, in conformità con i principi vigenti in materia di sicurezza digitale e protezione dei dati. L'utilizzo di detti mezzi, sia per le finalità previste dall'art. 128 del Regolamento suddetto, sia in generale in ambito formativo o culturale, è, però, regolato dalle norme del regime interno di ciascun istituto penitenziario, e alcune limitazioni possono essere stabilite individualmente negli stabilimenti carcerari secondo i termini dell'art. 128.

Il comma 2 dell'art. 129 dispone, infine, che l'uso del computer e delle apparecchiature informatiche – così come l'utilizzo di dispositivi esterni di archiviazione delle informazioni e la connessione alle reti di comunicazione – deve essere disciplinato dai relativi regolamenti interni.

In Francia[66], la legge del 15 agosto 2014 prevede che, a prescindere dalla durata della pena, i detenuti devono essere preordinati all'uscita dal carcere, in modo da ridurre il rischio di recidiva: tale

64. Ovvero il *service flamand pour l'emploi et la formation professionnelle*.

65. Il Regolamento penitenziario oggetto di analisi dispone all'art. 7, comma 4, che «il trasferimento dei dati di cui ai commi 2 e 3 del presente articolo sarà sempre effettuato in conformità con le disposizioni della legge organica n. 7 del 26 maggio 2021, sulla protezione dei dati personali trattati ai fini della prevenzione, accertamento, indagine e perseguimento dei reati e dell'esecuzione delle sanzioni penali». Infatti, il secondo comma del soprammenzionato articolo prevede che non è necessario il consenso del detenuto «per trasferire ad altre pubbliche amministrazioni, nell'ambito delle rispettive competenze, i dati personali contenuti negli archivi informatici penitenziari necessari affinché queste possano esercitare le loro funzioni nei confronti dei detenuti in materia dei servizi sociali, della previdenza sociale, dell'affidamento dei figli o simili»; il terzo comma dell'articolo 7 del Regolamento, invece, dispone che «i dati personali contenuti negli archivi informatici del carcere possono essere trasferiti anche senza previo consenso dell'interessato quando il trasferimento è destinato al Difensore civico o ad un istituto simile delle Comunità autonome che esercitano poteri esecutivi in materia penitenziaria, alla Procura della Repubblica o a un giudice o tribunali, nell'esercizio delle funzioni loro attribuite, nonché quando si tratta di trasferire dati personali relativi alla salute dei detenuti per motivi di urgenza o per effettuare studi ep*Ivi*iologici».

66. Come ricordato dal Presidente della Repubblica francese, Emmanuel Macron, nel discorso all'ENAP del 6 marzo 2018, un detenuto, benché privato della libertà, mantiene gli altri diritti, in quanto la vocazione stessa della pena è quella di reinserire il detenuto all'interno della società, nella quale egli deve, quindi, trovare il proprio spazio.

rischio può essere arginato dalla possibilità di trovare un lavoro[67] attraverso l'utilizzo di Internet[68].

Il *Défenseur des droits*, nel Rapporto relativo alla *Dématérialisation et inégalités d'accès aux services publics*, nel 2019 ha sottolineato che «in assenza di una connessione Internet, i detenuti non possono accedere ai propri diritti[69]».

Inoltre, il Difensore dei diritti francese – sentito, nel 2021, dalla commissione d'inchiesta dell'Assemblea nazionale volta ad individuare le disfunzioni e le carenze della politica penitenziaria francese – ha ricordato la necessità di rendere, all'interno degli istituti penitenziari, parte dei contenuti presenti su Internet liberamente accessibile attraverso siti web di servizi pubblici, organizzazioni sociali e siti di formazione online riconosciuti dal Ministero della Pubblica Istruzione. A tal fine, è stato messo in rilievo come sia imprescindibile porre in essere «un sostegno agli usi digitali e informatici per i detenuti e gli agenti penitenziari che ne hanno bisogno»[70].

L'articolo L413-1 del codice penitenziario francese, entrato in vigore il 1° maggio 2022, dispone che «le attività di formazione[71] generale o professionale vengono prese in considerazione per la valutazione della serietà degli sforzi di reinserimento e della buona condotta dei detenuti condannati. All'interno degli istituti penitenziari vengono assunte tutte le misure per fornire una formazione generale o professionale o la convalida dell'esperienza acquisita alle persone detenute che ne facciano richiesta» L'ultimo comma dell'articolo in esame prevede, poi, che i detenuti, «a tal fine, beneficiano dell'accesso alle risorse educative necessarie, anche digitali».

La *Commission Nationale Consultative des Droits de l'Homme*, nel suo *avis sur l'effectivité des droits fondamentaux en détention* del 24 marzo 2022, ha raccomandato un accesso sorvegliato a Internet affinché il diritto di reinserimento dei detenuti sia assicurato. Secondo la summenzionata Commissione, infatti, «l'accesso supervisionato a Internet consentirebbe di promuovere, non solo il mantenimento della vita privata e familiare, ma anche l'accesso all'informazione, alla cultura e alle procedure amministrative dematerializzate. Più in generale, consentirebbe di includere le persone detenute in una società connessa»[72].

Già nel 2009 erano state sperimentate in sette istituti penitenziari, nell'ambito di un accordo

67. In Francia, con la legge n. 87-432 del 22 giugno 1987, il lavoro, per i detenuti, si è trasformato dall'essere un obbligo a dare forma a un loro diritto.
68. Dal 1985, il servizio CLIP (*CLub Informatique Pénitentiaire*) si propone di sviluppare l'alfabetizzazione digitale dei detenuti.
69. Défenseur des droits 2019, p. 63.
70. Défenseur des droits 2021, p. 10.
71. L'art. 2 del Décret n. 2022-855 del 7 giugno 2022, ha abrogato, in vista dell'entrata in vigore del *Code pénitentiaire*, l'art. D436 del codice di procedura penale francese, il quale prevedeva che «l'istruzione primaria è fornita in tutti gli istituti penitenziari. I detenuti che non sanno leggere, scrivere o calcolare fluentemente devono beneficiare di questo impegno. Altri detenuti possono esservi ammessi su loro richiesta. Vengono organizzati corsi speciali per gli analfabeti e per coloro che non parlano né scrivono la lingua francese. Il regolamento interno determina tempi e modalità di detto insegnamento». Ad oggi, invero, l'art. L411-1 del codice penitenziario, dispone, in primo luogo, che «ogni persona detenuta condannata è tenuta a svolgere almeno una delle attività offerte dal capo dell'istituto penitenziario e dal direttore del servizio di integrazione e libertà vigilata, purché rivolte al suo reinserimento e adatte alla sua età, alle sue capacità, alla sua personalità e, nel caso, alla sua disabilità». In secondo luogo, la norma in esame precisa che «quando l'interessato detenuto non padroneggia gli insegnamenti fondamentali, l'attività consiste principalmente nell'apprendimento della lettura, della scrittura e del calcolo. Quando non padroneggia la lingua francese, l'attività consiste principalmente nell'impararla».
72. Commission Nationale Consultative des Droits de l'Homme 2022, p. 24. Nella Raccomandazione n. 9, in particolare, la Commissione, al fine di garantire il reinserimento delle persone detenute, pone l'attenzione sulla necessità di elaborare un percorso individuale di detenzione, di sviluppare l'offerta di attività fisiche, ricreative, culturali ed educative delle persone detenute e, infine, di permettere un accesso sorvegliato a Internet, tale da permettere il mantenimento dei legami con la società esterna alla realtà carceraria. Cfr. il parere oggetto di esame.

firmato nel 2007 tra il Ministero della Giustizia e la *Caisse des dépôts et consignations,* le *Cyber-bases justice*, ovvero spazi informatici dotati di reti con accesso limitato e controllato a Internet, privi della possibilità di interazione diretta con il mondo esterno. Si precisa, però, che alcuni di questi spazi a distanza di anni hanno cessato di funzionare a causa di una manutenzione insufficiente o inadeguata. In particolare, «durante la visita del carcere di Bordeaux-Gradignan nel luglio 2018, la *Cyber-base* non esisteva più. Presso il centro centrale di Saint-Martin-de-Ré, nel maggio 2017, è stato constatato che il sistema, divenuto obsoleto, presentava un numero crescente di malfunzionamenti. Nel centro penitenziario di Metz, visitato nel febbraio 2014, la *Cyber-base* soffriva della mancanza di aggiornamenti software e del browser. Le numerose difficoltà tecniche incontrate dal coordinatore sono state oggetto di segnalazioni comuni a tutte le *Cyber-bases*. Infine, nel centro penitenziario femminile di Rennes, ispezionato nel luglio 2015, è stato riferito che la *Cyber-base* era chiusa per motivi tecnici da marzo 2015»[73].

Al momento, il Ministero della giustizia è teso, dunque, ad attuare il nuovo progetto sperimentale *Numérique en détention* (Ned), per permettere ai detenuti di accedere a Internet – e, in particolare, a servizi preselezionati – tramite tablet condivisi. Tale progetto, intrapreso al precipuo scopo di permettere alle istituzioni di definire una strategia a livello nazionale, doveva debuttare nel 2019 nei centri penitenziari di Meaux, Nantes e nella casa circondariale di Dijon; in realtà, ha visto la luce solo in quest'ultimo nel 2021, oltre che nei siti di Melun e Strasburgo[74]. Segnatamente, in tali carceri i detenuti hanno la possibilità di contattare l'amministrazione penitenziaria attraverso una *saisine par voie électronique*, di acquistare generi alimentari e beni di uso quotidiano, di consultare il saldo del proprio conto personale e, infine, di avere accesso a un ambiente di lavoro digitale, sebbene limitato ad alcuni insegnamenti e formazioni e senza accesso a Internet.

Sulla base dell'indagine svolta, si può desumere che la concretizzazione, in positivo, di un accesso a Internet da parte dei detenuti, comporti dei costi significativi, sia con riferimento alle spese di gestione necessarie per rendere compatibile tale beneficio con la sicurezza pubblica, sia in relazione alle infrastrutture essenziali per la sua realizzazione; di qui, probabilmente, la scelta di declinare, in Francia, Belgio e Spagna, siffatto accesso come una libertà. Tuttavia, tale conformazione solleva delle perplessità in ordine alla sua compatibilità con la funzione rieducativa della pena; invero, un conto è riconoscere l'utilizzo di Internet da parte dei detenuti come un diritto sociale – quale in Finlandia e in Norvegia –, per, poi, subordinarlo, debitamente, alle scelte allocative delle risorse (rispetto alle quali esso potrebbe non essere una priorità), diverso è, di contro, individuarlo come libertà e, quindi, condizionarlo, in modo discrezionale, alle possibilità materiali e tecniche di ciascun istituto penitenziario.

5.2. L'accesso a Internet da parte dei detenuti come declinazione di un diritto sociale in Finlandia e in Norvegia

A differenza delle esperienze fin qui descritte, la Finlandia e la Norvegia disegnano l'accesso a Internet come un diritto sociale, che lo Stato è vincolato a garantire.

In Finlandia, il capitolo 12, sez. 9, dell'*Imprisonment Act* (767/2005), come emendato dalla legge n. 393/2015, prevede che a un detenuto può essere concesso il permesso di utilizzare Internet per una ragione importante legata al suo sostentamento o alla partecipazione ad attività lavorative, educative, giudiziarie, sociali o abitative, ovvero per un altro equivalente rilevante motivo.

Tale permesso, però, è soggetto a determinati presupposti: in primo luogo, il detenuto non può accedere ad altri siti web diversi da quelli indicati nell'autorizzazione; in secondo luogo, l'uso di Internet non deve mettere in pericolo l'ordine carcerario, la sicurezza e l'incolumità del carcere, nonché la sicurezza del detenuto o di altre persone. Il permesso, altresì, può essere revocato nel caso in cui tali presupposti non dovessero più essere soddisfatti dopo la decisione o se il detenuto violasse le condizioni del permesso. Dunque, in Finlandia, non solo l'accesso a Internet deve essere autorizzato, ma è anche asservito a una continua sorveglianza.

73. Cfr. Contrôleur général des lieux de privation de liberté, *Avis du 12 décembre 2019 relatif à l'accès à internet dans les lieux de privation de liberté*, in Journal Officiel de la République français, 6 febbraio 2020, p. 148.
74. Si precisa che tale progetto è stato sospeso nella prigione di Strasburgo.

Per quanto, invece, concerne più direttamente le comunicazioni elettroniche, la successiva sezione 9b dispone, in aggiunta a quanto previsto dall'*Information Society Code* (917/2014), che le autorità penitenziarie hanno il diritto, ove necessario, di recuperare i dati relativi all'invio e alla ricezione di una chiamata telefonica o di un messaggio sia dal dispositivo utilizzato dal detenuto per la comunicazione sia dai dispositivi e dai sistemi amministrati dal carcere per la trasmissione e l'elaborazione delle comunicazioni. In particolare, l'invio di messaggi di posta elettronica e l'utilizzo di Internet possono essere controllati mediante monitoraggio elettronico e con la presenza di un pubblico ufficiale del Servizio penitenziario e di libertà vigilata.

Malgrado ciò, l'inclusione digitale all'interno delle carceri trova un freno nelle lacune relative alle competenze informatiche dei detenuti[75]. In ragione di tale circostanza è stato sviluppato lo *Smart Prison Project* dalla *Finnish Criminal Sanctions Agency*, teso a promuovere l'inclusione digitale dei detenuti.

In Norvegia, parimenti, la sezione 3-20 del Capitolo 3 del *Forskrift om straffegjennomføring* – relativo alle norme sull'esecuzione delle sentenze – prevede che le apparecchiature informatiche e simili possono essere utilizzate dai detenuti per lavoro, istruzione[76] o altre misure solo quando tale uso è ritenuto appropriato rispetto alle condizioni locali e non è discutibile dal punto di vista della sicurezza. Le stesse regole valgono per l'uso di apparecchiature informatiche private. Nelle carceri di massima sicurezza, queste ultime possono essere consentite solo in situazioni formative molto specifiche in cui è documentata l'esigenza eccezionale atta a giustificarne l'impiego.

Come regola generale, i detenuti non possono utilizzare apparecchiature informatiche collegate ad una rete informatica esterna o apparecchiature informatiche esterne. Ciò, però, può avvenire, in primo luogo, qualora esista un motivo particolare che ne giustifichi il bisogno e, in secondo luogo, se ciò non ponga preoccupazioni dal punto di vista della sicurezza.

Tuttavia, la normativa sottolinea che il software e gli altri contenuti, sotto forma di testi, immagini, filmati o suoni, non devono essere tali da avere un effetto negativo sui detenuti stessi, sugli altri detenuti o sull'ambiente carcerario nel suo complesso.

Le norme relative alla corrispondenza elettronica sono, poi, stabilite nella sezione 3-27 del Regolamento anzidetto. Tale sezione prevede, infatti, che in circostanze eccezionali i detenuti possono essere autorizzati a utilizzare apparecchiature informatiche e altre apparecchiature elettroniche per comunicare con persone al di fuori del carcere. Siffatto *placet* è, tuttavia, sottoposto a una duplice condizione: il carcere deve poter monitorare[77] tali trasmissioni in conformità con le norme applicabili al controllo della posta e ciò deve poter essere attuato senza costi aggiuntivi.

6. Conclusioni

Dall'analisi svolta si apprezzano non pochi spunti di interesse comparatistico, che potrebbero, altresì, rivelarsi determinanti nella prospettiva di una possibile evoluzione del diritto italiano.

In primo luogo, a fronte dell'importanza che Internet ha assunto quale condizione di sviluppo della persona umana, non può ritenersi condivisibile l'opzione di vietare l'utilizzo di Internet all'interno degli istituti penitenziari. Dall'indagine

75. Sul punto, si veda, Järveläinen-Rantanen 2021, pp. 240-259. Gli autori, in particolare, sottolineano come «alcune persone intervistate hanno fatto una distinzione tra "millennial" e persone che hanno trascorso "30 anni in prigione"» (p. 249).

76. In ordine ai benefici di ricevere un'istruzione in prigione, si veda Tønseth-Bergsland 2019, pp. 1-13. Lo studio precisa che i detenuti norvegesi hanno un livello di istruzione inferiore alla media della popolazione: più della metà di essi possiede esclusivamente l'istruzione primaria. Invero, gli autori evidenziano che, essendo i detenuti «un gruppo complesso caratterizzato da un accumulo di problemi sociali», «uno degli obiettivi dell'educazione in carcere è fare qualcosa per risolvere questi problemi».

77. Tali comunicazioni possono essere monitorate leggendole integralmente, ascoltandole o vedendole prima di essere spedite dalla prigione o prima che il detenuto le riceva. Possono essere controllate anche le trasmissioni che il detenuto ha già ricevuto. Tuttavia, il contenuto delle comunicazioni elettroniche «da e verso un avvocato difensore nominato, diplomatici e altre persone specificate» non potrà essere letto, visto o ascoltato; in tal caso, infatti, il controllo può vertere esclusivamente in merito all'identità del mittente o del destinatario.

emerge, in secondo luogo, la necessità, non solo di non interdire tale accesso, ma anche di regolamentarlo in maniera espressa e per mezzo di norme primarie, risultando inadeguate fonti dissimili.

Le realtà statuali oggetto di studio – e la giurisprudenza della Corte EDU (in particolare, *Jankovskis c. Lithuania*) – sembrano, tuttavia, concordare che un siffatto accesso debba reggersi su un duplice assunto: la fruizione di Internet deve rivolgersi alla reintegrazione sociale e non può porsi in discordanza con le esigenze di sicurezza. Di qui, l'occorrenza di limitare l'accesso – anche attraverso la creazione di una piattaforma mediante la quale poter eseguire la consultazione – a determinati siti web che rispondano a peculiari finalità prefissate (relazionali, di studio, di lavoro, ecc.).

Appare, inoltre, evidente che gli ordinamenti che non approntano l'accesso a Internet come un diritto sociale, rimettendo ai singoli istituti penitenziari una piena discrezionalità in merito alla concretizzazione di tale diritto, si espongono a critiche in ordine al mancato rispetto, a parità di condizioni, del principio di uguaglianza.

L'inettitudine della soluzione che declina – in modo volontario o accidentale – come una libertà la fruizione di Internet in carcere, è dimostrata dal fatto che tanto il Belgio quanto la Francia stiano, all'interno di specifiche realtà carcerarie, sperimentando programmi volti a individuare soluzioni in grado di garantire un accesso – sicuro – a Internet da parte di persone private della libertà e idonee ad essere, in un secondo momento, estese a livello statuale; tuttavia, tali ordinamenti tardano a realizzare questi propositi a causa dei costi che una fruizione generalizzata comporterebbe.

L'ineccepibile rilevanza dell'aspetto economico di siffatto utilizzo, tuttavia, dovrebbe condurre non ad escludere la possibilità di individuare il diritto di accesso ad Internet in carcere come un diritto sociale, ma solo a subordinare quest'ultimo – una volta regolamentato – al bilanciamento delle «risorse finanziarie messe a disposizione per la protezione di tutti gli altri diritti sociali»[78].

Le esperienze della Finlandia e della Norvegia, infatti, mostrano come la fruizione di Internet in carcere, approntata come un diritto sociale, non solo appaia il modello più idoneo a livello teorico – in quanto laddove prevista, risponde in maniera ottimale alle finalità rieducative della pena –, ma sia in grado di essere realizzata sul piano pratico.

Riferimenti bibliografici

M.R. Allegri (2021), *Il diritto di accesso a Internet: profili costituzionali*, in "MediaLaws", 2021, n. 1

B. Arcangeli, P. Diana, F. di Mieri, G. Suriano (2010), *L'e-learning in carcere: una proposta*, in "Journal of e-Learning and Knowledge Society", 2010, n. 1, pp. 91-99

A. Baratta (2001), *Diritto alla sicurezza o sicurezza dei diritti?*, in S. Anastasia, M. Palma (a cura di), "La bilancia e la misura", FrancoAngeli, 2001

M. Bassini, O. Pollicino (a cura di) (2015), *Verso un Internet Bill of Rights*, Aracne, 2015

R. Bevilacqua (2015), *Le esperienze di e-democracy come aperture di spazi ristretti: carceri di Padova e Venezia*, in G. Gangemi (a cura di), "Dalle pratiche di partecipazione all'e-democracy. Analisi di casi concreti", Gangemi Editore, 2015

P. Bilancia (2011), *La complessa tutela dei diritti nella rete*, in A. Papa (a cura di), "Comunicazione e nuove tecnologie. New media e tutela dei diritti", Aracne, 2011

F. Borgia (2010), *Riflessioni sull'accesso a Internet come diritto umano*, in "La Comunità internazionale", n. 3, 2010, p. 395 ss.

78. Cfr. Tanzarella 2021, p. 54. L'autore, tuttavia, precisa di nutrire «molti dubbi nel considerare quello dell'accesso a Internet un diritto sociale fondamentale, preferendo piuttosto classificarlo come servizio pubblico universale necessario per il godimento di diritti fondamentali costituzionalmente previsti, da quelli individuali come le libertà di comunicazione e di pensiero, a quelli sociali come il diritto al lavoro, alla salute, all'istruzione» (p. 42).

G. Cassano, A. Contaldo (2009), *Internet e tutela della libertà di espressione*, Giuffrè, 2009

V.G. Cerf (2012), *Internet Access Is Not a Human Right,* in "New York Times", 4 gennaio 2012

Commission Nationale Consultative des Droits de l'Homme (2022), *Avis sur l'effectivité des droits fondamentaux en prison: du constat aux remèdes pour réduire la surpopulation carcérale et le recours à l'enfermements*, Parigi, Cedex, 24 marzo 2022

Contrôleur général des lieux de privation de liberté (2020), *Avis du 12 décembre 2019 relatif à l'accès à internet dans les lieux de privation de liberté*, in "Journal Officiel de la République française", 6 febbraio 2020

P. Costanzo (2015), *Internet e libertà d'informazione dentro le mura carcerarie*, in "Il diritto dell'informazione e dell'informatica", 2015, n. 6, pp. 949-950

P. Costanzo (1996), *Aspetti evolutivi del regime giuridico di Internet*, in "Il diritto dell'informazione e dell'informatica", 1996, n. 6, p. 831 ss.

L. Cuocolo (2012), *La qualificazione giuridica dell'accesso a Internet, tra retoriche globali e dimensione sociale*, in "Politica del diritto", 2012, n. 2-3, pp. 263-288

Défenseur des droits (2021), *Avis n. 21-13*, 30 settembre 2021

Défenseur des droits (2019), *Rapport - Dématérialisation et inégalités d'accès aux services publics*, Cedex, 2019

P. Diana (2013), *L'E-learning in carcere: esperienze, riflessioni e proposte*, in "Cambio. Rivista sulle trasformazioni sociali", 2013, n. 6

T.E. Frosini (2011), *Il diritto costituzionale di accesso a Internet*, in "AIC", 2011, n. 1, pp. 23-43

E. Järveläinen, T. Rantanen (2021), *Incarcerated people's challenges for digital inclusion in Finnish prisons*, in "Nordic Journal of Criminology", 2021, n. 2, pp. 240-259

M.C. Locchi, N. Pettinari (2020), *L'utilizzo di Skype in carcere al fine del mantenimento e del rafforzamento dei rapporti dei detenuti con il mondo esterno*, in "Archivio Penale", 2020, n. 1

F. Marcelli (2011), *L'accesso ad Internet come diritto fondamentale? Tendenze del diritto internazionale e realtà dei fatti*, in M. Pietrangelo (a cura di), "Il diritto di accesso ad internet", Atti della tavola rotonda svolta nell'ambito dell'IGF Italia 2010 (Roma, 30 novembre 2010), Edizioni Scientifiche Italiane, 2011

A. Menghini (2022), *Carcere e Costituzione. Garanzie, principio rieducativo e tutela dei diritti dei detenuti*, Editoriale Scientifica, 2022

F. Mollo (2022), *Internet e carcere nel sistema multilivello di tutela dei diritti fondamentali*, in "Rivista Italiana di Conflittologia", 2022, n. 45

P. Passaglia (2021), *La problematica definizione dell'accesso a Internet e le sue ricadute su esclusioni sociali e potenziali discriminazioni*, in "MediaLaws", 2021, n. 3

P. Passaglia (2014), *Internet nella Costituzione italiana: considerazioni introduttive*, in M. Nisticò, P. Passaglia (a cura di), "Internet e Costituzione", Atti del Convegno (Pisa, 21-22 novembre 2013), Giappichelli, 2014

M. Reglitz (2020), *The Human Right to Free Internet Access*, in "Journal of Applied Philosophy", vol. 37, 2020, n. 2

S. Rodotà (2015-a), *Il diritto di avere diritti*, Laterza, 2015

S. Rodotà (2015), *Prefazione*, in L. Manconi, G. Torrente (a cura di), "La pena e i diritti", Carocci, 2015

S. Rodotà (2010), *Una Costituzione per Internet?*, in "Politica del diritto", 2010, n. 3, pp. 337-351

M. Ruotolo (2022), *Diritti dei detenuti e Costituzione*, Giappichelli, 2022

M. Ruotolo (2022), *Il sistema penitenziario e le esigenze della sua innovazione*, in "BioLaw Journal", 2022, n. 4

P. Tanzarella (2021), *L'accesso a Internet è fondamentale, ma è davvero un diritto (fondamentale)?*, in "MediaLaws", 2021, n. 1

C. Tønseth, R. Bergsland (2019), *Prison education in Norway – The importance for work and life after release*, in "Cogent Education", vol. 6, 2019, n. 1

A. Valastro (2011), *Le garanzie di effettività del diritto di accesso a Internet e la timidezza del legislatore italiano*, in M. Pietrangelo (a cura di), "Il diritto di accesso ad internet", Atti della tavola rotonda svolta nell'ambito dell'IGF Italia 2010 (Roma, 30 novembre 2010), Edizioni Scientifiche Italiane, 2011

F. Wilhelmsson, G. Jackson, O. Makne (2017), *How can ICT make the offender better prepared for release?*, EUROPRIS, 2017

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0150 • articolo sottoposto a peer review • pubblicato in anteprima il 10 giu. 2024

Valeria Pietrella – Stefania Racioppi

Il *credit scoring* e la protezione dei dati personali: commento alle sentenze della Corte di giustizia dell'Unione europea del 7 dicembre 2023

L'articolo analizza le sentenze della Corte di giustizia dell'Unione europea del 7 dicembre 2023 (cause riunite C-26/22 e C-64/22 e C-634/21). Le decisioni offrono infatti l'opportunità di riflettere su due temi principali: l'ampiezza del sindacato giurisdizionale esercitato su una decisione di reclamo adottata da un'autorità di controllo e la liceità della raccolta e del trattamento, anche automatizzato, dei dati personali. Le forme di tutela connesse al trattamento dei dati personali, sviluppandosi in più livelli e con modalità differenti, delineano nel loro complesso un sistema volto a garantire la massima protezione dei dati, che, anche in un'ottica di bilanciamento degli interessi, appare – almeno alla luce delle sentenze in esame – prevalere sugli interessi commerciali connessi all'utilizzo degli stessi.

Corte di giustizia dell'Unione europea – Credit scoring – Protezione dei dati personali
Sindacato giurisdizionale – Trattamento automatizzato

Credit scoring and personal data protection: comment on the judgments of the Court of Justice of the European Union Dec. 7, 2023

The article analyzes the judgments of the Court of Justice of the European Union of December 7, 2023 (Joined Cases C-26/22 and C-64/22 and C-634/21). These decisions give the opportunity to reflect on two main issues: the range of judicial review exercised over a complaint decision adopted by a supervisory authority and the lawfulness of the collection and processing of personal data, including automated processing. The forms of protection related to the processing of personal data, by developing at different levels and in different ways, outline as a whole a system aimed at ensuring the highest level of data protection, which, also from a balancing of interests perspective, appears – at least in accordance with the judgments under consideration – to prevail over the commercial interests related to the use of the data.

Court of Justice of the European Union – Credit scoring – Personal data protection – Judicial review
Automated data processing

Le Autrici sono dottorande di ricerca del XXXVIII ciclo presso Sapienza – Università di Roma, curriculum diritto amministrativo. I paragrafi 1 e 3 sono a cura di V. Pietrella; i paragrafi 2, 4, 4.1, 4.2, 4.3 sono a cura di S. Racioppi

1. Premessa. I fatti all'origine delle questioni pregiudiziali

Con due sentenze del 7 dicembre 2023 la Corte di giustizia dell'Unione europea si è pronunciata su questioni inerenti alla disciplina sulla protezione dei dati personali di cui al Regolamento generale sulla protezione dei dati (RGPD) con riferimento alla conservazione e all'utilizzo dei dati da parte di società private che forniscono informazioni commerciali.

In particolare, con tali sentenze la Corte si è pronunciata su due domande di pronuncia pregiudiziale sollevate dal *Verwaltungsgericht Wiesbaden* (Tribunale amministrativo di Wiesbaden, Germania) nell'ambito di controversie sorte in merito al rifiuto dello *Hessischer Beauftragter für Datenschutz und Informationsfreiheit* (di seguito "HBI"), il Commissario per la protezione dei dati e la libertà di informazione del Land dell'Assia, di ingiungere alla SCHUFA Holding AG (di seguito "SCHUFA"), società che si occupa di valutazione dei crediti, di procedere alla soppressione e alla cancellazione di dati conservati da quest'ultima.

La prima delle sentenze in esame, relativa alle cause riunite C-26/22 e C-64/22, riguarda le controversie relative a due soggetti che nell'ambito di procedure di insolvenza hanno ottenuto un'esdebitazione anticipata sulla base di ordinanze giudiziarie. In accordo con la disciplina di diritto tedesco in materia, la pubblicazione ufficiale su Internet di tali decisioni era stata cancellata dopo sei mesi dalla rispettiva data di adozione (art. 3, par. 1 InsoBekV).

Tuttavia, tali informazioni erano ancora presenti nelle banche dati detenute dalla SCHUFA in quanto quest'ultima sopprime le informazioni solo dopo tre anni dalla registrazione, sulla base di un codice di condotta elaborato dall'associazione che riunisce le società che forniscono informazioni commerciali in Germania, approvato dall'Autorità di controllo competente.

I soggetti interessati hanno pertanto richiesto alla SCHUFA di cancellare le iscrizioni relative alle decisioni di esdebitazione di cui erano stati oggetto. La SCHUFA ha rigettato la richiesta, ritenendo la sua attività conforme alla disciplina prevista dal RGPD e di non essere soggetta all'applicazione del termine di cancellazione di sei mesi.

Dunque, i soggetti interessati hanno proposto un reclamo all'HBDI, l'Autorità di controllo competente, la quale, con decisioni, rispettivamente, del 1° marzo 2021 e del 9 luglio 2021, ha ritenuto lecito il trattamento dei dati effettuato dalla SCHUFA.

Avverso tali decisioni i soggetti interessati hanno presentato ricorso dinanzi al Tribunale amministrativo di Wiesbaden. Nell'ambito di tali procedimenti sono emerse alcune questioni relative in particolare alla natura giuridica della decisione emanata dall'Autorità di controllo a seguito di un reclamo ai sensi dell'art. 77, par. 1, RGPD, e al sindacato del giudice su tale decisione, nonché in relazione alla liceità della conservazione, presso le società che forniscono informazioni commerciali, di dati in merito alla solvibilità di una persona provenienti da registri pubblici e alla durata di tale conservazione.

Con le decisioni del 23 dicembre 2021 e del 31 gennaio 2022, il Tribunale amministrativo di Wiesbaden ha sospeso i predetti giudizi e proposto alla Corte cinque questioni pregiudiziali,

trattate dalla Corte di giustizia riassumendole nelle seguenti questioni:

i) «se l'articolo 78, paragrafo 1, del RGPD debba essere interpretato nel senso che il controllo giurisdizionale esercitato su una decisione su reclamo adottata da un'autorità di controllo si limita a stabilire se tale autorità abbia trattato il reclamo, adeguatamente indagato sull'oggetto di quest'ultimo e informato il reclamante della conclusione dell'esame, o se tale decisione debba essere oggetto di un sindacato giurisdizionale completo, compreso il potere del giudice adito di imporre all'autorità di controllo di adottare una misura concreta» (prima questione);

ii) «se l'articolo 5, paragrafo 1, lettera a), del RGPD, in combinato disposto con l'articolo 6, paragrafo 1, primo comma, lettera f), di tale regolamento, debba essere interpretato nel senso che osta a una prassi di una società che fornisce informazioni commerciali, consistente nel conservare, nelle proprie banche dati, informazioni provenienti da un registro pubblico relative alla concessione di esdebitazioni a favore di persone fisiche, e nel cancellare tali informazioni al termine di un periodo di tre anni, conformemente a un codice di condotta ai sensi dell'articolo 40 del medesimo regolamento, mentre il periodo di conservazione di dette informazioni nel registro pubblico è di sei mesi, e se l'articolo 17, paragrafo 1, lettere c) e d), del RGPD debba essere interpretato nel senso che una società che fornisce informazioni commerciali, che abbia ripreso informazioni relative alla concessione di esdebitazioni da un pubblico registro, è tenuta a cancellarle» (questioni dalla seconda alla quinta).

Con riferimento alla prima questione, la Corte ha concluso che «l'articolo 78, paragrafo 1, del RGPD deve essere interpretato nel senso che una decisione su reclamo adottata da un'autorità di controllo è soggetta a un sindacato giurisdizionale completo» (par. 70).

Per quanto riguarda le questioni dalla seconda alla quinta, trattate congiuntamente, la Corte ha poi concluso che «l'articolo 5, paragrafo 1, lettera a), del RGPD, in combinato disposto con l'articolo 6, paragrafo 1, primo comma, lettera f), di tale regolamento, dev'essere interpretato nel senso che osta ad una prassi di società che forniscono informazioni commerciali consistente nel conservare, nelle proprie banche dati, informazioni provenienti da un registro pubblico relative alla concessione di esdebitazioni a favore di persone fisiche, al fine di poter fornire informazioni sul merito creditizio di tali persone, per un periodo che va oltre quello durante il quale i dati sono conservati nel registro pubblico», che «l'articolo 17, paragrafo 1, lettera c), del RGPD deve essere interpretato nel senso che l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione, senza ingiustificato ritardo, dei dati personali che lo riguardano qualora si opponga al trattamento ai sensi dell'articolo 21, paragrafo 1, di tale regolamento e non sussistano motivi legittimi prevalenti che possano giustificare, in via eccezionale, il trattamento in esame», e che «l'articolo 17, paragrafo 1, lettera d), del RGPD deve essere interpretato nel senso che il titolare del trattamento è tenuto a cancellare, senza ingiustificato ritardo, i dati personali oggetto di un trattamento illecito» (par. 113).

Il secondo caso, relativo alla causa C-634/21, riguarda invece l'attività di calcolo dei punteggi ("scoring") operata dalla SCHUFA sulla probabilità di un comportamento futuro di un soggetto sulla base di caratteristiche di tale soggetto, attraverso procedure matematiche e statistiche.

In particolare, la vicenda riguardava un soggetto al quale era stata negata la concessione di un prestito da parte di un terzo a seguito di informazioni negative redatte dalla SCHUFA e trasmesse a quest'ultimo.

Ritenendo errati i dati comunicati, il soggetto interessato aveva richiesto alla SCHUFA di consentirgli di comunicare le informazioni corrette sui dati personali registrati e di cancellare quelle errate.

Dopo aver informato il soggetto del livello del suo punteggio e, a grandi linee, delle modalità di calcolo, la SCHUFA ha riscontrato negativamente la richiesta presentata, invocando il segreto commerciale e affermando che essa si limitava a far pervenire informazioni alle sue controparti contrattuali, lasciando a queste ultime le decisioni contrattuali propriamente dette.

Il soggetto interessato ha pertanto presentato reclamo all'HBDI, chiedendo di ingiungere alla SCHUFA di accogliere la sua domanda di accesso alle informazioni e di cancellazione.

Con decisione del 3 giugno 2020, l'Autorità di controllo ha respinto tale domanda, ritenendo

non dimostrato che la SCHUFA non rispettasse i requisiti previsti dalla legge federale sulla protezione dei dati, *Bundesdatenschutzgesetz* (BDSG) e, in particolare, l'art. 31 in materia di protezione delle operazioni economiche in caso di "scoring" e di informazioni sulla solvibilità.

Il soggetto interessato ha dunque proposto ricorso avverso tale decisione dinanzi al Tribunale amministrativo di Wiesbaden.

Al fine di statuire sulla controversia, il Tribunale tedesco ha ritenuto necessario determinare se il calcolo di un tasso di probabilità come quello di specie costituisca un processo decisionale automatizzato relativo alle persone fisiche, ai sensi dell'art. 22, par. 1, con la conseguenza che, in tal caso, la liceità di tale attività sarebbe subordinata alla condizione che tale decisione sia autorizzata dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento (art. 22, par. 2, lett. b), RGPD).

Il giudice di rinvio ha dunque sospeso il procedimento e sottoposto alla Corte di giustizia le seguenti questioni pregiudiziali:

i) «se l'articolo 22, paragrafo 1, del [RGPD] debba essere interpretato nel senso che il calcolo automatizzato di un tasso di probabilità relativo alla capacità di un interessato di saldare in futuro un debito costituisce già una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produce effetti giuridici che riguardano l'interessato o che incide in modo analogo significativamente sulla sua persona, qualora tale tasso, calcolato sulla base di dati personali relativi all'interessato, sia trasmesso dal titolare del trattamento a un terzo titolare del trattamento e quest'ultimo basi prevalentemente su tale tasso la sua decisione sulla stipulazione, sull'attuazione o sulla cessazione di un contratto con l'interessato»;

ii) in caso di risposta negativa alla prima questione, «se l'articolo 6, paragrafo 1, e l'articolo 22 del [RGPD] debbano essere interpretati nel senso che ostano a una normativa nazionale ai sensi della quale il ricorso a un tasso di probabilità – nella fattispecie relativo alla solvibilità e alla disponibilità a pagare di una persona fisica, che includa informazioni sui crediti – di un certo comportamento futuro di una persona fisica, allo scopo di decidere sulla stipulazione, sull'attuazione o sulla cessazione di un contratto con tale persona ("scoring"), è consentito solo se sono soddisfatte determinate ulteriori condizioni, meglio specificate nella motivazione della domanda di pronuncia pregiudiziale».

Per quanto riguarda la prima questione, la Corte ha concluso che «l'articolo 22, paragrafo 1, del RGPD deve essere interpretato nel senso che il calcolo automatizzato, da parte di una società che fornisce informazioni commerciali, di un tasso di probabilità basato su dati personali relativi a una persona e riguardanti la capacità di quest'ultima di onorare in futuro gli impegni di pagamento costituisce un "processo decisionale automatizzato relativo alle persone fisiche", ai sensi di tale disposizione, qualora da tale tasso di probabilità dipenda in modo decisivo la stipula, l'esecuzione o la cessazione di un rapporto contrattuale con tale persona da parte di un terzo, al quale è comunicato tale tasso di probabilità» (par. 73).

Avendo risposto in modo affermativo a tale questione, la Corte non si è pronunciata sulla seconda.

2. Introduzione ai temi giuridici

Le decisioni in commento offrono l'opportunità di riflettere su due temi principali, da un lato l'ampiezza del sindacato giurisdizionale esercitato su una decisione di reclamo adottata da un'autorità di controllo, dall'altro la liceità della raccolta e del trattamento dei dati personali.

In via preliminare sembra opportuno osservare come alle suddette questioni faccia da sfondo il principio del bilanciamento tra gli interessi in gioco[1]. I casi affrontati riguardano infatti la SCHUFA,

1. Il bilanciamento degli interessi è contenuto nel Considerando 4 del RGPD, laddove si specifica che «il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato» in ottemperanza al principio di proporzionalità «con altri diritti fondamentali», tra i quali sono espressamente menzionati il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica. Si aggiunga che la dottrina ha nel tempo individuato ulteriori

una società privata di diritto tedesco che fornisce ai suoi partner contrattuali informazioni commerciali sul merito creditizio di soggetti terzi, soprattutto consumatori, registrate e archiviate nelle proprie banche dati. Se è comprensibile l'esigenza dei prestatori di servizi e beni di conoscere i propri clienti e i rischi connessi ai vincoli contrattuali in procinto di assumere[2], non si può trascurare il bisogno di tutela che deve essere garantito agli interessati laddove vengano utilizzati anche metodi automatizzati nel trattamento dei propri dati personali.

Tale tutela si estrinseca non soltanto nell'assicurare un controllo pieno in sede giurisdizionale, ma altresì nell'esercizio da parte degli stessi interessati dei diritti riconosciuti dal RGPD, quali quelli di cancellazione e di non sottoposizione ad una decisione basata unicamente sul trattamento automatizzato dei dati.

3. Sul sindacato giurisdizionale

La prima questione sollevata nelle sentenze in esame riguarda la portata del sindacato del giudice sulle decisioni adottate da un'autorità di controllo su un reclamo, ai sensi dell'art. 78, par. 1 del Regolamento 679/2016 – RGPD.

Nel caso di specie, l'HBDI aveva infatti interpretato il diritto di presentare un reclamo, previsto all'art. 77, par. 1, del Regolamento, come un mero diritto di petizione, rispetto al quale il controllo giurisdizionale si limiterebbe a verificare che l'autorità di controllo abbia trattato il reclamo e abbia informato l'autore dello stato e dell'esito dello stesso, senza esaminare nel merito la correttezza della decisione emanata dall'autorità.

Tale argomentazione era stata messa in dubbio dal giudice del rinvio, il quale, in particolare, aveva rilevato il rischio che una simile interpretazione potesse compromettere l'effettività del ricorso giurisdizionale, garantita dall'art. 78, par. 1, del Regolamento, nonché porsi in contrasto con gli obiettivi di quest'ultimo, anche nel quadro dell'attuazione degli articoli 7 e 8 della Carta, in materia di rispetto della vita privata e della vita familiare e della protezione dei dati di carattere personale.

In particolare, la procedura di reclamo di cui trattasi è disciplinata dall'art. 77 del predetto Regolamento, il quale prevede il «diritto di proporre reclamo a un'autorità di controllo» per «l'interessato che ritenga che il trattamento che lo riguarda violi il […] regolamento».

Il successivo art. 78 dispone poi che «Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ogni persona fisica o giuridica ha il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda».

Tale disposizione fa dunque espressamente riferimento a una tutela giurisdizionale effettiva, ponendo quale unica condizione che quest'ultima riguardi una «decisione giuridicamente vincolante».

A tal riguardo, la Corte di giustizia ha ritenuto che le decisioni adottate dall'HBDI costituiscono decisioni giuridicamente vincolanti, tenuto conto dei poteri esercitati da tale autorità nonché in accordo con quanto stabilito dal considerando 143 del Regolamento, secondo il quale il rifiuto o il rigetto di un reclamo da parte di un'autorità di controllo costituisce una decisione che produce effetti giuridici nei confronti del reclamante.

Pertanto, richiamandosi alla sentenza del 12 gennaio 2023 (C132/21), la Corte ha considerato che dall'art. 78, par. 1, del RGPD, letto alla luce del considerando 143, discende che i giudici investiti di un ricorso avverso una decisione di un'autorità di controllo dovrebbero disporre della piena competenza e, in particolare, di quella a esaminare

diritti fondamentali, «alla luce dei quali bilanciare la protezione dei dati personali anche nell'ottica della valutazione delle misure di sicurezza da adottare, l'ordine e la sicurezza pubblica, l'attività di prevenzione e repressione dei reati, la tutela della salute e – laddove il trattamento sia effettuato da una PA – l'interesse alla celerità, alla trasparenza e all'efficacia dell'attività amministrativa», così Finocchiaro 2017, p. 21.

2. Si tratta, in concreto, degli articoli 18 e 21 della direttiva 2014/17/UE del Parlamento europeo e del Consiglio, del 4 febbraio 2014, in merito ai contratti di credito ai consumatori relativi a beni immobili residenziali e recante modifica delle direttive 2008/48/CE e 2013/36/UE e del regolamento (UE) n. 1093/2010, e degli articoli 8 e 9 della direttiva 2008/48/CE del Parlamento europeo e del Consiglio, del 23 aprile 2008, relativa ai contratti di credito ai consumatori e che abroga la direttiva 87/102/CEE.

tutte le questioni di fatto e di diritto relative alla controversia ad essi sottoposta[3].

Pertanto, il controllo giurisdizionale esercitato su tale decisione non potrebbe limitarsi alla questione se l'autorità di controllo abbia trattato il reclamo, indagato in modo adeguato sull'oggetto di quest'ultimo e informato il reclamante della conclusione dell'esame, ma, al contrario «affinché un ricorso giurisdizionale sia "effettivo", come richiesto da tale disposizione, una siffatta decisione deve essere sottoposta ad un sindacato giurisdizionale completo»[4].

Tale interpretazione sarebbe corroborata dagli obiettivi e dalle finalità perseguiti dal Regolamento, il quale mira ad assicurare un elevato livello di protezione delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione[5], nonché dagli ampi poteri attribuiti all'autorità di controllo ai sensi dell'art. 58 predetto Regolamento, il quale conferisce a tale autorità significativi poteri di indagine al fine di porre rimedio alla violazione delle disposizioni del Regolamento, prevedendo diverse misure correttive.

Alla luce di tali poteri, la Corte ha dunque concluso che l'esigenza di una tutela giurisdizionale effettiva non sarebbe soddisfatta se le decisioni adottate da tali autorità fossero soggette solo a un sindacato giurisdizionale ristretto.

Le pronunce della Corte risultano coerenti anche con le finalità di armonizzazione della disciplina tra gli Stati membri, enunciate ai considerando 10 e ss. del Regolamento.

Del resto, come rilevato nel considerando 6 del Regolamento, a causa della rapidità dell'evoluzione tecnologica e della globalizzazione «la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo», consentendo tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali con estrema facilità. All'esito di tali trasformazioni, la tecnologia dovrebbe quindi «facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali».

A oggi i dati personali sono dunque caratterizzati da una dimensione necessariamente sovranazionale e, pertanto, l'esigenza di una regolazione e protezione omogenea degli stessi nei diversi Stati membri risulta particolarmente necessaria.

Inoltre, le sentenze offrono interessanti spunti di riflessione anche con riferimento al sindacato del giudice sulle decisioni di altre autorità indipendenti. Quella del sindacato sui provvedimenti discrezionali delle autorità indipendenti ha costituito infatti una questione molto dibattuta in dottrina e in giurisprudenza, tenuto conto delle caratteristiche di tali autorità, dotate di alta competenza tecnica ed esperienza[6].

Anzitutto, occorre rilevare che il trattamento dei dati personali costituisce un caso particolare. Infatti, nel nostro ordinamento, ai sensi dell'art. 152, d.lgs. n. 196/2003 (Codice della privacy) la giurisdizione sui provvedimenti emanati dall'autorità di controllo italiana, il Garante per la protezione dei dati personali, è attribuita al giudice ordinario. Ne deriva che non sussistono i medesimi limiti che si porrebbero con riguardo al sindacato del giudice amministrativo.

Ad ogni modo, secondo il Regolamento gli Stati Membri possono scegliere diversi mezzi di tutela purché ciò non comporti l'esercizio di un sindacato con una portata diversa a seconda del giudice adito.

Al contrario, si avrebbe infatti la conseguenza che per uno stesso caso, a seconda che la violazione del Regolamento sia stata posta in essere in uno Stato membro o in un altro, e dunque i soggetti si siano trovati a presentare reclamo dinanzi alle autorità di controllo di uno Stato membro o di un altro, le decisioni emanate da tali autorità sarebbero sottoposte a un controllo più o meno intenso.

Ciò risulta particolarmente rilevante anche tenuto conto che l'art. 77 del predetto Regolamento consente di adire sia l'autorità del luogo ove si è

3. CGUE, 7 dicembre 2023, C26/22 e C64/22, par. 52.
4. CGUE, 7 dicembre 2023, C26/22 e C64/22, par. 53.
5. Cfr. conss. 10 e 11 del Regolamento 679/2016-GDPR.
6. *Ex multis* Corte di Cassazione, Sez. Un., 7 maggio 2019, n. 11929; Cons. Stato, sez. VI, 30 gennaio 2020, n. 780; Lazzara 2002; Merusi 2002; Cintioli 2005; Moliterni 2022, p. 209 ss.

realizzata la violazione sia l'autorità del luogo ove lo stesso è residente.

In questa prospettiva, nelle sentenze in esame si può cogliere una tendenza della Corte di giustizia ad ammettere, se necessaria, un'estensione del sindacato sulle decisioni delle autorità indipendenti, rispetto alle quali si rileva infatti che «le garanzie di indipendenza non sono punto compromesse dal fatto che le decisioni giuridicamente vincolanti di un'autorità di controllo sono soggette ad un sindacato giurisdizionale completo»[7].

L'affermazione si pone peraltro in continuità con la giurisprudenza più recente della Corte di giustizia sull'intensità del sindacato del giudice sui provvedimenti fondati su valutazioni tecniche, con riguardo agli atti adottati dalle istituzioni europee[8]. Tale giurisprudenza sembrerebbe infatti operare un sindacato sempre più ampio anche con riferimento a tali decisioni, seppure adottate da autorità dotate di amplissima discrezionalità.

Ebbene, anche in questo caso è possibile osservare una simile tendenza. Infatti, quanto ai limiti del predetto sindacato, la Corte precisa che, sebbene il giudice nazionale disponga di una «piena competenza per esaminare tutte le questioni di fatto e di diritto relative alla controversia di cui trattasi», ciò non implica che «esso sia legittimato a sostituire la sua valutazione della scelta delle misure correttive appropriate e necessarie a quella di tale autorità, ma esige che tale giudice esamini se l'autorità di controllo abbia rispettato i limiti del suo potere discrezionale»[9].

Sembrerebbe dunque che il giudice non potrebbe entrare nel merito delle scelte compiute dall'autorità, in quanto discrezionali.

Tuttavia, come si vedrà, nel fornire precisazioni intese a guidare il giudice del rinvio, la stessa Corte di giustizia sembrerebbe operare un sindacato particolarmente intenso. Ciò conferma, pertanto, la completezza del sindacato ammesso, la quale nel contesto in esame appare inevitabilmente connessa anche alle peculiari esigenze relative alla protezione dei dati, al centro della disciplina in oggetto.

4. Sul trattamento dei dati. Questioni generali

Le questioni successive affrontate dalla Corte di Giustizia nella sentenza relativa alle cause riunite C-26/22 e C-64/22 e poi, meglio riprese, nella sentenza C-634/21, attengono propriamente al trattamento dei dati personali in relazione alle norme del Regolamento 679/2016 (RGPD).

Ai fini di un corretto inquadramento normativo, prima di procedere alla disamina delle disposizioni del RGPD, appare doveroso ricordare che il legislatore europeo, già nelle direttive 2008/48/CE e 2014/17/UE, invitava i creditori a valutare il merito di credito del consumatore prima di erogare un credito, al fine di migliorare le condizioni per l'instaurazione e il funzionamento del mercato interno.

Secondo quanto previsto dalla Direttiva 2014/17, la valutazione del merito di credito avviene sulla base di informazioni riguardanti la situazione economico-finanziaria del consumatore, reddito e spese comprese, le quali possono essere ottenute da varie fonti[10]. A tale scopo ai sensi dell'articolo 21 «ciascuno Stato membro garantisce a tutti i creditori l'accesso di tutti gli Stati membri alle banche dati utilizzate nello Stato membro in questione per valutare il merito creditizio dei consumatori e al solo scopo di verificare che i consumatori rispettino gli obblighi di credito per tutta la durata del contratto di credito. Le condizioni di tale accesso non sono discriminatorie».

La valutazione del merito creditizio è dunque effettuata dai creditori, i quali, al fine di evitare distorsioni della concorrenza, dovrebbero poter accedere a tutte le banche dati relative ai crediti, private o pubbliche, contenenti dati relativi ai consumatori. Tuttavia, l'esistenza in parallelo di banche dati di natura pubblica e privata genera il rischio di una possibile concorrenza di sistemi

7. CGUE, 7 dicembre 2023, C26/22 e C64/22, par. 65.
8. CGUE, 4 maggio 2023, C-389/2021; Trib. UE, 10 maggio 2023, T34/21 e T87/21.
9. CGUE, 7 dicembre 2023, C26/22 e C64/22, par. 69.
10. Le Linee guida dell'Autorità bancaria europea sull'origine e il monitoraggio dei prestiti (EBA/GL/2020/06) indicano quali categorie di dati possono essere utilizzate per il trattamento dei dati personali ai fini della valutazione del merito creditizio.

sottoposti a regimi giuridici differenti e dunque, di conflitti legali. Come evidenziato dall'Avvocato Generale nelle conclusioni presentate alla Corte di giustizia il 16 marzo 2023, «le differenze normative possono divenire particolarmente problematiche se incidono sulla protezione dei dati, poiché, a prescindere dal soggetto, pubblico o privato, che tiene il registro, questi deve rispettare, nel modo in cui detti dati sono gestiti e registrati, l'interesse delle persone coinvolte»[11]. Tale assunto appare inoltre avvalorato dal fatto che l'attività dei gestori delle banche dati private è di solito disciplinata da codici di condotta, conformemente all'articolo 40, par. 1 e 2 del RGPD.

Le fattispecie da cui originano le questioni pregiudiziali sollevate dal Tribunale tedesco forniscono perciò l'opportunità alla Corte di Lussemburgo di pronunciarsi sulle prassi delle agenzie di valutazione del credito alla luce delle disposizioni del Regolamento europeo in materia di protezione di dati personali, onde valutarne la conformità ai principi di liceità, di limitazione delle finalità, di minimizzazione dei dati.

4.1. Sulla cancellazione dei dati personali in caso di "conservazione multiforme di dati"

La prima questione affrontata nelle cause riunite C-26/22 e C-64/22 riguarda la compatibilità con gli articoli 5, 6 e 17 del RGPD della conservazione di dati trasferiti da registri pubblici – e da questi ultimi cancellati, stante la scadenza del termine legalmente prevista – in banche dati di una società privata senza uno specifico motivo, ma al solo fine di poter fornire informazioni in caso di un'eventuale richiesta dei partner commerciali.

In ordine al trattamento dei dati che implichi una "conservazione multiforme dei dati", non solo in un registro pubblico, ma anche nelle banche dati delle società che forniscono informazioni commerciali, la Corte di giustizia, nel richiamare i propri precedenti, osserva che «la presenza degli stessi dati personali in più fonti rafforza l'ingerenza nel diritto della persona alla vita privata»[12]. Difatti, più le informazioni sono facilmente accessibili al pubblico, più è forte l'ingerenza nei diritti fondamentali dell'interessato, di cui agli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea. Pertanto, nonostante la meritevolezza degli interessi del settore creditizio a disporre delle informazioni necessarie a fondare un rapporto di fiducia, non può essere giustificato un trattamento dei dati personali oltre il termine di conservazione dei dati nel registro pubblico fallimentare. In altri termini «la conservazione di tali dati da parte di una società che fornisce informazioni commerciali non può essere fondata sull'articolo 6, paragrafo 1, primo comma, lettera f), del RGPD per quanto riguarda il periodo successivo alla cancellazione di detti dati da un registro pubblico fallimentare»[13] (par. 99). Ne consegue che, nel caso di un trattamento dei dati personali effettuato oltre il termine di conservazione dei dati di sei mesi nel registro pubblico fallimentare, l'interessato avrebbe il diritto di ottenere dal titolare del trattamento la cancellazione, senza ingiustificato ritardo, ai sensi dell'articolo 17 paragrafo 1, lettera d), del RGPD (parr. 107 e 108).

Mentre per quanto riguarda il periodo di sei mesi nel corso del quale i dati in questione sono disponibili in entrambi i registri, la Corte di giustizia afferma che spetta al giudice del rinvio «ponderare gli interessi in gioco e gli effetti sull'interessato, al fine di stabilire se la conservazione parallela di tali dati da parte di società che forniscono informazioni commerciali possa essere considerata limitata allo stretto necessario» (par. 100). In tale

11. Conclusioni dell'Avvocato Generale Priit Pikamäe presentate il 16 marzo 2023 nelle Cause riunite C26/22 e C64/22, par. 32.
12. La Corte richiama la sentenza del 4 luglio 2023, *M.P. e a.* (Condizioni generali di utilizzo di un social Network), C-252/21, par. 106; ma cfr. anche Sentenza del 1° agosto 2022, *Vyriausioji tarnybinės etikos komisija* (C-184/20, par. 92).
13. Ai sensi dell'articolo 6 paragrafo 1, primo comma, lettera f), del RGPD affinché il trattamento di dati personali sia lecito è necessario che ricorrano tre condizioni cumulative: «in primo luogo, il perseguimento del legittimo interesse da parte del titolare del trattamento o di un terzo, in secondo luogo, la necessità del trattamento dei dati personali per la realizzazione del legittimo interesse perseguito e, in terzo luogo, la condizione che gli interessi o i diritti e le libertà fondamentali dell'interessato dalla tutela dei dati non prevalgano».

evenienza, ove il giudice del rinvio dovesse concludere per la conformità del trattamento rispetto all'articolo 6, paragrafo 1, primo comma, lettera f), del RGPD, troverebbe applicazione l'articolo 17, paragrafo 1, lettera c), così interpretato dalla Corte: «l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione, senza ingiustificato ritardo, dei dati personali che lo riguardano qualora si opponga al trattamento ai sensi dell'articolo 21, paragrafo 1, di tale regolamento e non sussistano motivi legittimi prevalenti che possano giustificare, in via eccezionale, il trattamento in esame».

Tale ultimo passaggio della pronuncia in esame merita di essere approfondito alla luce delle seguenti considerazioni. Come noto, i dati personali devono essere trattati nel rispetto dei principi di liceità, correttezza e trasparenza, oltre che di proporzionalità, declinata nei corollari di "minimizzazione dei dati" e di "limitazione della conservazione" in forza dei quali gli stessi devono essere raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo compatibile con tali finalità, ma anche limitati a quanto necessario rispetto alle finalità per le quali sono trattati[14]. La Corte di giustizia invita quindi il giudice *a quo* a ponderare gli interessi in gioco, posto che il numero di utenti che potrebbe avere accesso ai dati degli interessati nel termine di conservazione nel registro pubblico rischia di essere veramente elevato. Ciò in quanto, sebbene i dati siano già disponibili nei registri pubblici, la circostanza per cui gli stessi siano anche conservati e resi disponibili in parallelo nelle banche dati di società private di valutazione del credito assume un impatto maggiore sulla vita delle persone. Infatti, «L'informazione non deve solo essere disponibile, ma anche opportunamente gestita/trattata»[15].

Tale riflessione può essere meglio espressa mutando l'angolo di visuale. La Corte di giustizia richiama una famosa pronuncia del 2014 nella quale ha statuito che «un trattamento inizialmente lecito di dati esatti può divenire, con il tempo, incompatibile con la direttiva suddetta qualora tali dati non siano più necessari in rapporto alle finalità per le quali sono stati raccolti o trattati» (punto 93)[16]. Nel caso *Google Spain e Google*, la Corte di giustizia ha affermato che il gestore di un motore di ricerca è obbligato a eliminare, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, i link verso pagine web pubblicate da terzi e contenenti informazioni relative a tale persona, anche quando detta pubblicazione sia di per sé lecita, prima di procedere, in un secondo momento, al bilanciamento dei diritti dell'interessato con l'interesse economico del gestore del motore di ricerca e, altresì, con l'interesse del pubblico ad accedere all'informazione in questione (punto 88). Eppure è stato osservato come essendo «generalmente riconosciuto che, ove un'informazione sia lecita, la persona che la diffonde beneficia in ogni caso della libertà di espressione sancita all'articolo 11 della Carta, sarebbe stato utile che la Corte avesse espressamente menzionato tale diritto fondamentale»[17]. Anche la Corte europea dei diritti dell'uomo, in alcune pronunce recenti[18], ha ribadito il principio di cui all'articolo 8 della CEDU per cui i dati personali sottoposti a trattamento automatizzato devono essere conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore a quello strettamente necessario. A tal fine il titolare del trattamento è chiamato periodicamente a valutare se la conservazione dei dati personali sia ancora necessaria e a riconoscere all'interessato il diritto alla cancellazione dei dati nel caso in cui la necessità sia venuta meno. L'interessato ai sensi degli artt. 17, par. 1, lett. c) e 21, par. 1 RGPD può opporsi al trattamento dei dati, esercitando il diritto alla cancellazione degli stessi. Il titolare dovrà quindi astenersi dal trattare i dati personali, salva la dimostrazione dell'esistenza di motivi legittimi imperativi prevalenti.

Il tema appare di spiccato interesse in forza della invalsa attività svolta di *web scraping*, ossia di

14. Art. 5, Regolamento 679/2016 – RGPD.
15. Ponti 2023, p. 117.
16. Sentenza Corte di giustizia 13 maggio 2014, *Google Spain e Google*, C-131/12.
17. Conclusioni dell'Avvocato generale Maciej Szpunar, presentate il 10 gennaio 2019, nella causa C507/17, *Google LLC contro Commission nationale de l'informatique et des libertés (CNIL)*.
18. Cfr. Corte EDU, Sez. III, 16 aprile 2024 (n. 40519/15) – *T. c. Bulgaria.*

raccolta massiva di dati personali a fini di addestramento degli algoritmi di intelligenza artificiale (IA) da parte di soggetti terzi[19]. Il Garante della protezione dei dati personali italiano, ritenendo sussistente una lesione dei diritti degli interessati, ha sanzionato una società che aveva sviluppato un sistema di riconoscimento facciale che sfruttava un database di immagini raccolte da fonti online pubbliche tramite tecniche di *web scraping*[20]. Così il principio di trasparenza che dovrebbe guidare le amministrazioni e, in generale il settore pubblico, diviene un obiettivo non semplice da perseguire «a fronte di processi automatizzati che divengono sempre più strutturalmente, tecnologicamente opachi»[21].

4.2. Sui codici di condotta

Le problematiche legate alla cancellazione delle informazioni creditizie erano già state sollevate in dottrina. Preliminarmente veniva suggerita la distinzione tra il diritto alla cancellazione, che sorge allorquando l'ipotesi di segnalazione sia erronea o illegittima e il diritto a non vedere conservata un'informazione pregiudizievole per un periodo di tempo illimitato dopo che ne siano venuti meno i presupposti[22]. Si metteva poi in evidenza come le diverse tempistiche previste per l'eliminazione di diverse tipologie di dati all'interno di ciascuno Stato membro e tra gli stessi non assicurasse una parità di trattamento fra i diversi consumatori europei[23].

La pronuncia in esame appare dunque suggestiva anche in ordine a quanto statuito circa la natura giuridica dei codici di condotta. A livello normativo si richiama l'articolo 40 del RGPD in virtù del quale le associazioni e gli altri organismi rappresentanti le categorie di titolari o responsabili del trattamento possano elaborare (modificare o prorogare) codici di condotta destinati a contribuire alla corretta applicazione del Regolamento in specifici settori di attività e in funzione delle particolari esigenze delle micro, piccole e medie imprese, successivamente approvati dall'Autorità Nazionale di controllo competente.

In Germania – nel caso esaminato dalla Corte – le associazioni di categoria avevano proposto – e l'Autorità competente aveva approvato – un codice di condotta nel quale si stabilivano termini di cancellazione eccedenti rispetto ai termini di conservazione previsti per i registri pubblici. Sul punto sembra opportuno riportare le parole dell'Avvocato Generale, secondo il quale «un siffatto codice di condotta rappresenta solo un impegno volontario di chi lo ha elaborato e adottato, vale a dire dell'associazione succitata e dei suoi membri. Parimenti, il fatto che detto codice di condotta sia stato approvato da un'autorità di controllo significa unicamente che quest'ultima, quale autorità amministrativa, si considera vincolata ad esso. Tuttavia, mi sembra evidente che esso è privo di efficacia vincolante nei confronti dei terzi in ragione del principio "pacta tertiis nec nocent nec prosunt"». Pertanto, le agenzie di valutazione del credito, in qualità di titolari del trattamento, «non possono trincerarsi dietro le regole del codice di condotta che esse stesse hanno elaborato per validamente sottrarsi agli obblighi derivanti a loro carico da tale regolamento».

Ne deriva, come affermato dalla Corte di giustizia, che allorquando il codice di condotta sfoci in una valutazione diversa da quella ottenuta in applicazione dell'articolo 6, paragrafo 1, primo comma, lettera f), del RGPD «non può essere preso in considerazione nella ponderazione effettuata in forza di tale disposizione» (par. 105).

Anche in Italia, oltre alla Centrale dei Rischi (CR), un archivio gestito dalla Banca d'Italia per finalità di interesse pubblico[24], esistono i Sistemi di

19. Così il Garante per la protezione dei dati personali che ha avviato un'indagine sulla raccolta di dati personali on line per addestrare gli algoritmi. L'iniziativa è volta a verificare l'adozione di misure di sicurezza da parte di siti pubblici e privati, 22 novembre 2023.
20. Garante per la protezione dei dati personali, *Ordinanza ingiunzione nei confronti di Clearview AI*, 10 febbraio 2022 [doc. web n. 9751362].
21. Carloni 2023, p. 220.
22. Cfr. sul punto Frigeni 2013, p. 365 ss.
23. Così Buonanno 2022, pp. 588-589.
24. La Centrale dei Rischi è stata istituita con la delibera CICR del 16 maggio 1962 e regolamentata dalla delibera CICR del 29 marzo 1994, nonché dalla Circolare n. 139 dell'11 febbraio 1991 s.m.i. Il suo fondamento normativo

Informazioni Creditizie (SIC)[25], ossia banche dati private alle quali gli intermediari partecipano su base volontaria. Nella Relazione del Garante della privacy per l'anno 2022 si legge che il flusso di reclami e segnalazioni in materia di trattamenti di dati personali censiti nei sistemi di informazioni creditizie gestiti da soggetti privati «è stato estremamente intenso»[26]. Per la risoluzione dei reclami, il Garante ha richiamato le norme contenute nel codice di condotta[27], nel quale in ordine ai tempi di conservazione si stabilisce che «le informazioni creditizie di tipo negativo relative a inadempimenti non successivamente regolarizzati possono essere conservate nel SIC non oltre trentasei mesi dalla data di scadenza contrattuale del rapporto oppure, in caso di altre vicende rilevanti in relazione al pagamento, dalla data in cui è risultato necessario il loro ultimo aggiornamento, e comunque, anche in quest'ultimo caso, al massimo fino a sessanta mesi dalla data di scadenza del rapporto, quale risulta dal contratto»[28]. Tuttavia sembra opportuno rilevare che mentre nella Centrale dei Rischi i dati «sono conservati per il tempo necessario al perseguimento delle finalità istituzionali» e comunque comunicati agli intermediari bancari e finanziari per le finalità connesse con l'assunzione e la gestione del rischio di credito limitatamente agli ultimi 36 mesi; nei sistemi di informazioni creditizie il termine è fissato dall'art. 7 del Codice deontologico e dall'allegato 2 in maniera diversa a seconda dei casi e comunque sino ad un periodo massimo di 60 mesi.

5. Sul trattamento automatizzato dei dati

Il caso trattato nella seconda sentenza esaminata (C-634/21) riguarda invece l'interpretazione dell'articolo 22 del RGPD, dal titolo *Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione*[29]. Come già evidenziato in narrativa, il ricorrente, non avendo ottenuto un credito a causa di una valutazione di solvibilità effettuata dalla SCHUFA, chiedeva a quest'ultima di consentirgli di accedere ai dati registrati che lo riguardavano e di cancellare quelli inesatti. La SCHUFA tuttavia, nell'opporre il segreto professionale, industriale e aziendale, comunicava al privato

è rintracciabile negli artt. 51, comma 1 e 53, comma 1 lett. b) TUB relativo ai poteri di vigilanza della Banca d'Italia. In dottrina sul servizio per la centralizzazione dei rischi bancari si v. Liace 2007, p. 112 ss.; Sciarrone Alibrandi 2005, p. 1 ss.; in giurisprudenza la C.R. è stata definita «uno strumento di ausilio per gli intermediari per la valutazione del merito creditizio della clientela e, in generale, per l'analisi e la gestione del relativo rischio, attraverso il quale si persegue l'obiettivo di accrescere la stabilità del sistema» (cfr. Cass. civ., sez. I, 25 gennaio 2017, n. 1931, Cass. civ., sez. I, 29 gennaio 2015, n. 1725, Cass. civ., sez. III, 16 dicembre 2014, n. 26361; Cass. civ., sez. I, 12 ottobre 2007, n. 21428).

25. Costituiscono esempi di Sistemi di Informazione Creditizia: Crif Eurisc, Experian, CTC, Assilea.

26. Garante per la Protezione dei Dati Personali 2022.

27. Il Garante lo definisce «strumento di autoregolamentazione ad adesione volontaria in grado di concorrere alla corretta applicazione della normativa in materia di protezione dei dati personali (art. 40)». È stato adottato con il provvedimento del Garante della Privacy del 6 ottobre 2022, n. 324.

28. All.to 2 del Codice di condotta.

29. Art. 22 RGPD ai sensi del quale «1. 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. 2.Il paragrafo 1 non si applica nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) 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; c) si basi sul consenso esplicito dell'interessato. 3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e gli interessi legittimi 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. 4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato».

soltanto il punteggio di scoring calcolato nei suoi confronti e, in termini generali, il funzionamento del suo calcolo, senza indicare il peso riconosciuto nel calcolo ai diversi dati.

L'articolo 22 del RGPD, da leggere alla luce del considerando 71 del medesimo Regolamento, prevede il "diritto" dell'interessato di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione[30] che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. La disposizione *de qua* riconosce dunque che il processo decisionale automatizzato possa avere conseguenze gravi per gli interessati. La terminologia impiegata tuttavia appare estremamente generica, pertanto proprio la portata delle restrizioni di cui all'articolo 22 del RGPD costituisce l'oggetto della questione pregiudiziale esaminata dalla Corte di giustizia.

In dottrina infatti era stato osservato come il diritto dell'interessato a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato risultasse in concreto facilmente "aggirabile"[31]. Tra le eccezioni dell'articolo 22, par. 2 del RGPD è infatti previsto che il trattamento automatizzato sia ammesso ove necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento, proprio come nel caso di un contratto bancario.

Attraverso un'interpretazione ampia della nozione di "decisione", la Corte di giustizia ricomprende nel divieto di cui all'articolo 22 RGPD anche il risultato del calcolo della solvibilità di una persona sotto forma di tasso di probabilità relativo alla capacità di onorare impegni di pagamento in futuro, quando sia in grado di incidere in maniera significativa nella sfera giuridica dell'interessato, come nel caso del rifiuto ad una richiesta di concessione di prestito[32].

La decisione automatizzata, cui la normativa sulla tutela dei dati personali fa riferimento, non è soltanto una decisione in senso stretto, ma anche qualsivoglia tipologia di atto volta ad incidere sulla persona interessata. Lo *scoring* effettuato dalla SCHUFA non può dunque essere paragonato alla stregua di un atto preparatorio rispetto alla decisione assunta da un soggetto terzo di concedere o meno un prestito, come aveva sostenuto la Corte Federale di Giustizia tedesca[33]. Se così fosse infatti, non sarebbe garantito all'interessato l'esercizio del diritto ad accedere ai suoi dati personali in quanto l'istituto mutuante, non avendo svolto l'attività di *credit scoring*, non avrebbe a sua disposizione le informazioni richieste.

Come rilevato dall'Avvocato Generale «l'assenza di una definizione legale consente di desumere che il legislatore dell'Unione abbia optato per una nozione ampia, idonea a ricomprendere una molteplicità di atti che possono incidere sull'interessato in diversi modi»[34]. Nelle Linee Guida del Gruppo di Lavoro articolo 29 n. WP251 erano già state poste le basi per un'interpretazione più estensiva. Viene infatti affermato che l'espressione "basata unicamente su un trattamento automatizzato" debba riferirsi ad una decisione presa in assenza di una «qualsiasi effettiva influenza sul risultato» da parte di chi l'ha adottata. Solo laddove vi sia un significativo controllo sulla decisione da parte di qualcuno che abbia l'autorità e la competenza di cambiare la decisione si può escludere l'applicazione delle previsioni del RGPD in materia di processi decisionali automatizzati. L'art. 22 par. 1 vieta

30. Ai sensi dell'articolo 4, punto 4, del RGPD «Ai fini del presente regolamento s'intende per: (…) 4) "profilazione": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali 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».
31. Bagni 2021, nota 20, p. 915.
32. Parr. 46-48 della sentenza in commento (C-634).
33. *Bundesgerichtshof*, 28 gennaio 2014, VI ZR 156/13, par. 22. La Corte espressamente concludeva che nei casi in cui il processo automatizzato è limitato alla preparazione degli elementi da considerare e il merito della decisione finale di concedere il credito è valutato da una persona reale, il sistema non rientra nell'ambito del regime di protezione dei dati.
34. Punto 38 delle conclusioni dell'Avvocato Generale Priit Pikamäe, presentate il 16 marzo 2023.

in conclusione l'adozione di decisioni prese senza il coinvolgimento di un essere umano che possa influenzare ed eventualmente modificare il risultato mediante la sua autorità o competenza. La *ratio* della norma va ricercata nella tutela delle persone fisiche dagli effetti potenzialmente discriminatori e iniqui dei trattamenti automatizzati dei dati, tale da estendere l'ambito di applicazione della disposizione a tutte le decisioni in cui le prove preparatorie e i giudizi discrezionali sono completamente basati su mezzi automatizzati anche qualora un essere umano prenda formalmente la decisione[35].

L'interpretazione estensiva della nozione di decisione implica nuove considerazioni in tema di responsabilità legate sia alle "azioni" di macchine non supervisionate in modo continuativo, sia all'impiego delle risultanze di tali strumenti. Natalino Irti sul legame fra decisione e responsabilità ricorda che «vivere è scegliere, e perciò assumere su di sé il rischio e la responsabilità di una decisione. Non occorrono filosofie esistenzialistiche; basta anche una pallida e lieve coscienza di sé. Ogni situazione di vita ci interpella, ci chiama alla risposta, a sciogliere dilemmi e alternative. In tutte, o quasi tutte, le parole, che servono a descrivere la trama dell'esistenza, c'è la radice "duo": due o più sono le soluzioni, dinanzi a cui si trova la nostra volontà. Donde "dubbî", "dualismi", "dilemmi", che lacerano l'animo, e chiedono di essere sciolti nella risolutezza di una decisione. Ecco un'altra parola fondamentale. Decidere, che ci viene dal latino "decaedere", e significa troncare, toglier via, e quindi sgombrare il cammino e andare oltre»[36].

È stato osservato che per comprendere a fondo il tema occorre «mettere a fuoco il processo che è alla base del meccanismo decisorio e come questo si leghi al concetto di responsabilità»[37]. In primo luogo è necessario studiare il modello decisionale di volta in volta impiegato, in quanto anche il più semplice, consistente nell'azione di scegliere fra due alternative, implica una decisione e dunque una responsabilità. Tuttavia nella realtà i processi decisionali dell'intelligenza artificiale possono essere molto complessi e talora opachi, tali da non consentire l'interpretazione e la comprensione delle risultanze raggiunte. La poca trasparenza rende difficile stabilire quali cause hanno prodotto un determinato risultato ai fini dell'imputazione di una responsabilità. Al fine di superare l'opacità degli algoritmi divengono cruciali i principi di spiegabilità e della necessaria imputabilità della decisione ad una persona fisica, posto che tali concetti sono «interdipendenti e reciprocamente rafforzanti: senza una spiegabilità adeguata, attribuire la responsabilità per le azioni di un sistema di AI può diventare un problema estremamente complesso»[38].

La rilevanza della connessione tra la spiegabilità e i requisiti di legittimità della decisione automatizzata è stata di recente oggetto di una pronuncia della Corte di Cassazione. Il caso affrontato dalla Suprema Corte nell'ordinanza n. 14381 del 25 maggio 2021 riguardava il trattamento dei dati personali funzionale alla determinazione del profilo reputazionale dei soggetti. «Il problema, per la liceità del trattamento, era invece (ed è) costituito dalla validità – per l'appunto – del consenso che si assume prestato al momento dell'adesione. E non può logicamente affermarsi che l'adesione a una piattaforma da parte dei consociati comprenda anche l'accettazione di un sistema automatizzato, che si avvale di un algoritmo, per la valutazione oggettiva di dati personali, laddove non siano resi conoscibili lo schema esecutivo in cui l'algoritmo si esprime e gli elementi all'uopo considerati»[39].

Ne deriva che la scarsa trasparenza dell'algoritmo impedisce il formarsi di un valido consenso in tema di trattamento dei dati personali, che al contrario presuppone la consapevolezza di chi lo esprime che a sua volta deve comprendere la conoscenza dello "schema esecutivo dell'algoritmo".

Tornando alla pronuncia in esame, si osservi come la possibilità di ricorrere a sistemi automatizzati di *credit scoring*, basati non solo su modelli matematici e statistici, ma anche su tecnologie avanzate di artificial intelligence e machine

35. Malgeri-Comandè 2017.

36. Irti 2021, p. 73.

37. Carcaterra 2024, p. 44.

38. Marchetti Spaccamela-Silvestri 2024, p. 168; sul punto, cfr. anche Lo Sapio 2021.

39. Corte di Cassazione civile, sez. I, ordinanza, 25 maggio 2021, n. 14381.

learning, sia stata oggetto di un recente studio della Banca d'Italia. In quest'ultimo è stato evidenziato come l'adozione di modelli di AI-ML per il *credit scoring* comporti un incremento della possibilità che la selezione dei clienti risulti distorta rispetto all'effettiva rischiosità, configurando anche possibili forme di discriminazione[40]. Pertanto, in conformità con il Regolamento (UE) n. 575/2013 relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento, l'Autorità di vigilanza invita gli intermediari a disporre «un processo per vagliare i dati immessi nel modello di previsione che contempli una valutazione dell'accuratezza, completezza e pertinenza dei dati»[41]. Inoltre segnala l'esigenza che gli intermediari combinino «il modello statistico con la valutazione e la revisione umana in modo da verificare le assegnazioni effettuate in base al modello e da assicurare che i modelli siano utilizzati in modo appropriato». La *ratio* è proprio quella di far sì che l'intermediario sia in condizioni di scoprire e limitare gli errori derivanti da carenze del modello. L'indagine condotta dalla Banca d'Italia evidenzia come i modelli di intelligenza artificiale di *credit scoring*, nella maggioranza dei casi, siano alimentati da dati di provenienza interna ovvero acquistati da fornitori di *analytics* attivi nel mercato del credito e solo raramente da dati provenienti da web o social media. Alcuni intermediari hanno poi indicato di avere intenzione in futuro di ridurre progressivamente l'intervento umano all'interno del processo di concessione del credito, favorendo, ad esempio, la concessione di credito in forma automatizzata in caso di valutazione positiva da parte del modello.

In dottrina sul punto è emersa l'esigenza di raccordare il principio di sana e prudente gestione con il principio di prestito responsabile, in quanto se «l'emersione normativa della valutazione di merito creditizio importa una diretta incidenza sui rapporti con la clientela, anche la sua fase prodromica – quale quella del *credit scoring* – deve essere idonea a garantire un'attenzione adeguata alle peculiarità degli stessi e alle esigenze di protezione del singolo soggetto finanziato»[42]. Il principio viene ricondotto all'obbligo del finanziatore di predisporre tutte le misure necessarie per prevenire e monitorare il rischio di bias dell'IA e di opacità del processo. Ciò, come visto, in tanto potrà avvenire in quanto i modelli di intelligenza artificiale siano accompagnati da un certo grado di spiegabilità.

Da ultimo valga rilevare che le affermazioni dalla Corte di giustizia nella sentenza in commento appaiono in linea anche con quanto previsto dal Regolamento sull'intelligenza artificiale[43]. Stante l'elevato impatto sulla vita degli individui e il rischio di introdurre o perpetuare dinamiche di discriminazione nella valutazione dell'affidabilità creditizia delle persone, i sistemi IA di *credit scoring* sono infatti classificati come ad alto rischio. Il considerando 58 stabilisce che «È inoltre opportuno classificare i sistemi di IA utilizzati per valutare il merito di credito o l'affidabilità creditizia delle persone fisiche come sistemi di IA ad alto rischio, in quanto determinano l'accesso di tali persone alle risorse finanziarie o a servizi essenziali quali l'alloggio, l'elettricità e i servizi di telecomunicazione. I sistemi di IA utilizzati a tali fini possono portare alla discriminazione fra persone o gruppi e possono perpetuare modelli storici di discriminazione, come quella basata sull'origine razziale o etnica, sul genere, sulle disabilità, sull'età o sull'orientamento sessuale, o possono dar vita a nuove forme di impatti discriminatori».

In conclusione, qualora un soggetto faccia ricorso a sistemi di intelligenza artificiale per il *credit scoring*, fatte salve le garanzie previste dal RGPD, sarà tenuto anche al rispetto delle norme previste dall'AI Act in materia di sistemi ad alto rischio, così come previsto anche dalla Proposta di Direttiva relativa ai crediti al consumo ai sensi della quale «data l'alta posta in gioco, ogniqualvolta la valutazione del merito creditizio comporti un

40. Bonaccorsi di Patti-Calabresi-De Varti et al. (2021).

41. Articolo 174 CRR – Regolamento europeo 575/2013.

42. Rabitti 2023, p. 198.

43. Regolamento sull'intelligenza artificiale, Risoluzione legislativa del Parlamento europeo del 13 marzo 2024 sulla 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)0206 – C9-0146/2021 – 2021/0106(COD)), doc. P9_TA(2024)0138.

trattamento automatizzato, il consumatore dovrebbe avere il diritto di ottenere l'intervento umano da parte del creditore o dei fornitori di servizi di credito tramite crowdfunding. Il consumatore dovrebbe inoltre avere il diritto di ottenere una spiegazione significativa della valutazione effettuata e del funzionamento del trattamento automatizzato applicato, compresi, fra l'altro, le principali variabili, la logica e i rischi inerenti, come pure il diritto di esprimere la propria opinione e di contestare la valutazione del merito creditizio e la decisione»[44].

6. Conclusioni

Dall'analisi delle sentenze della Corte di giustizia emerge un'efficace ricostruzione delle peculiari tutele connesse al trattamento dei dati personali.

Tali forme di tutela si sviluppano infatti su più livelli e con modalità diverse, delineando nel loro complesso un sistema volto a garantire la massima protezione dei dati, che, anche in un'ottica di bilanciamento degli interessi, appare prevalere sugli interessi commerciali connessi all'utilizzo degli stessi.

Dall'analisi delle questioni sopra descritte è infatti possibile individuare molteplici forme di protezione dei dati, tra loro interconnesse e complementari, che si estrinsecano nel riconoscimento di particolari diritti ai soggetti interessati, come quello di presentare reclami e di ottenere la cancellazione dei dati che li riguardano, nell'attribuzione di poteri significativi all'autorità di controllo, e, infine, nel riconoscimento di un sindacato giurisdizionale completo sulle decisioni emanate da tale autorità.

L'intensità di tali tutele emerge in modo particolare dal caso di specie anche nella contrapposizione con interessi commerciali rilevanti quali gli interessi del settore creditizio a disporre delle informazioni necessarie a fondare un rapporto di fiducia.

Le questioni esaminate aprono infine a numerosi interrogativi. Infatti, a fronte della continua evoluzione delle tecnologie digitali e dell'incremento dell'impiego degli algoritmi in numerosi settori, occorre interrogarsi sulle possibili conseguenze delle pronunce in esame con particolare riferimento all'applicabilità dei concetti espressi dalla Corte anche ad altri casi di trattamento automatizzato dei dati.

Inoltre, l'interpretazione estensiva della nozione di decisione, applicata nella giurisprudenza in esame, implica altresì nuove considerazioni con riferimento al tema della responsabilità, particolarmente rilevante a fronte dell'opacità che caratterizza la natura dell'algoritmo.

Infine, ulteriori interrogativi sul punto si pongono con riferimento alla prossima attuazione dell'AI Act, che sembrerebbe completare il quadro di garanzie predisposto dal RGPD.

Riferimenti bibliografici

F. Bagni (2021), *Uso degli algoritmi nel mercato del credito: dimensione nazionale ed europea*, in "Osservatorio sulle fonti", 2021, n. 2

E. Bonaccorsi di Patti, F. Calabresi, B. De Varti et al. (2021), *Intelligenza artificiale nel credit scoring. Analisi di alcune esperienze nel sistema finanziario italiano*, Banca d'Italia, Questioni di Economia e Finanza (Occasional Papers), n. 721, ottobre 2021

L. Buonanno (2022), *Un modello giuridico europeo di credit reporting industry*, in "Banca borsa titoli di credito", 2022, n. 4

A. Carcaterra (2024), *La responsabilità nella decisione degli agenti artificiali ed umani*, in A. Lalli (a cura di), "La regolamentazione pubblica delle tecnologie digitali e dell'intelligenza artificiale", Giappichelli, 2024

44. Considerando 48 della Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa ai crediti al consumo Bruxelles, 30 giugno 2021 COM(2021) 347 2021/0171; cfr. anche considerando 48 dell'*AI Act*.

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 Giuridica, 2023

F. Cintioli (2005), *Giudice amministrativo, tecnica e mercato*, Giuffrè, 2005

G. Finocchiaro (2017), *Il quadro d'insieme sul Regolamento europeo*, in G. Finocchiaro (a cura di), "Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali", Zanichelli, 2017

C. Frigeni (2013), *Segnalazioni presso le centrali rischi creditizie e tutela dell'interessato: profili evolutivi*, in "Banca borsa titoli di credito", 2013, n. 4

Garante per la Protezione dei Dati Personali (2022), *Relazione annuale*, 2022

N. Irti (2021), *Inizio e Obbedienza*, in "Criminalia", 2021

P. Lazzara (2002), *Autorità indipendenti e discrezionalità*, Cedam, 2002

G. Liace (2007), *Centrale rischi*, in "Digesto delle Discipline Privatistiche. Sezione Commerciale", IV ed., Utet giuridica, 2007

G. Lo Sapio (2021), *La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione*, in "federalismi.it", 2021, n. 16

G. Malgeri, G. Comandè (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

A. Marchetti Spaccamela, F. Silvestri (2024), *Trasparenza e interpretabilità delle decisioni dei sistemi di Intelligenza Artificiale*, in A. Lalli (a cura di), "La regolamentazione pubblica delle tecnologie digitali e dell'intelligenza artificiale", 2024

F. Merusi (2002), *Giustizia amministrativa e autorità amministrative indipendenti*, in "Diritto amministrativo", 2002, n. 2

A. Moliterni (2022), *Autorità indipendenti e controllo giurisdizionale. L'esperienza italiana in prospettiva comparata*, in "Liber amicorum per Marco D'Alberti", Giappichelli, 2022

B. Ponti (2023), *Attività amministrativa e trattamento dei dati personali. Gli standard di legalità tra tutela e funzionalità*, FrancoAngeli, 2023

M. Rabitti (2023), Credit scoring *via* machine learning *e prestito responsabile*, in "Rivista di diritto bancario", 2023, n. 1

A. Sciarrone Alibrandi (2005), *La rilevazione centralizzata dei rischi creditizi: ricostruzione evolutiva del fenomeno e crescita degli interessi*, in Id. (a cura di), "Centrale rischi. Profili civilistici", Giuffrè, 2005

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0141 • articolo sottoposto a peer review • pubblicato in anteprima il 13 giu. 2024

Favorita Barra

Il diritto d'accesso civico generalizzato (c.d. FOIA): paradigmi, modelli e percorsi applicativi

Il contributo analizza la normativa italiana sul diritto di accesso civico generalizzato (c.d. FOIA) nel quadro di alcuni modelli ed esperienze maturate a livello europeo ed extraeuropeo. Oltre alla disciplina sulla libertà di informazione prevista dall'ordinamento giuridico italiano, lo scritto prende in esame la normativa sulla "libertà di informazione" adottata in Svezia, Francia, Spagna e infine negli Stati Uniti d'America. Dalla matrice comune delle normative prese in considerazione risaltano i tratti differenziali, legati al *core* di ogni ordinamento giuridico, alla sua storia costituzionale e al naturale processo evolutivo di valori e criteri direttivi.

Trasparenza – Libertà di informazione – Diritto ad essere informati – Accesso – Accessibilità – Informazioni Dati – Documenti

The right of generalised civic access (so-called FOIA): paradigms, models and application paths

The contribution analyzes the Italian legislation on the right of generalised civic access (so-called FOIA) within the framework of some models and experiences developed in European and non-European legal systems. In addition to the regulations on freedom of information provided by the Italian legal system, the paper examines the legislation on "freedom of information" adopted in Sweden, France, Spain, and in the United States of America. From the common matrix of the regulations under consideration, the differential traits stand out, linked to the core of each legal system, its constitutional history, and the natural evolutionary process of values and guiding criteria.

Transparency – Freedom of information – Right to be informed – Access – Accessibility – Information – Data Documents

L'Autrice è professoressa incaricata di Informatica giuridica e collaboratrice alla didattica dei corsi Diritto dell'amministrazione digitale e Macchine intelligenti e diritto alla Luiss Guido Carli; è consulente presso il FormezPA Presidenza del Consiglio dei Ministri – Dipartimento della Funzione pubblica

1. Introduzione

L'accesso agli atti amministrativi come riflesso e articolazione del principio della trasparenza, contribuisce a delineare un nuovo modo di essere e di agire della pubblica amministrazione.

Superata l'asimmetria nella relazione di potere tra i cittadini e l'apparato pubblico, le modalità attraverso cui la pubblica amministrazione opera sono rese conoscibili e decifrabili, al fine di rendere l'amministrazione una vera e propria "casa di vetro".

Le pagine che seguono avranno ad oggetto l'analisi della normativa italiana sull'accesso civico generalizzato nel quadro di alcuni modelli ed esperienze che si sono affermate a livello europeo ed extraeuropeo.

Come è noto, il decreto legislativo 25 maggio 2016, n. 97 – che concorre a integrare e a riformare la disciplina prevista dal decreto legislativo 14 marzo 2013, n. 33, riguardante il diritto di accesso civico, gli obblighi di pubblicità, la trasparenza e la diffusione di informazioni da parte delle pubbliche amministrazioni – ha innestato nel sistema giuridico italiano un diritto a conoscere riconducibile ai paradigmi della libertà di informazione. Da un lato, vengono ridimensionati, sia pure con misura, gli obblighi di pubblicità, dall'altro, viene introdotto un "diritto a conoscere generalizzato".

L'accesso civico generalizzato è inserito in un contesto normativo articolato: esso va ad affiancare non solo l'accesso civico, di cui costituisce formalmente una declinazione, ma anche il diritto di accesso documentale o "difensivo", che il legislatore ha scelto di non modificare.

Proprio l'eccessiva frammentazione formale e sostanziale delle regole sul diritto di accesso, che si riversa sul profilo del coordinamento tra i contenuti e sulla concreta regolamentazione dei procedimenti, è considerata uno dei nodi critici della normativa italiana[1].

1. L'istituto dell'accesso è variegato, oltre alle forme già indicate nel preambolo introduttivo, si distinguono, per il carattere della specialità: l'accesso agli atti e alle informazioni degli enti locali, attualmente disciplinato dal d.lgs. 18 agosto 2000, n. 267 (Testo unico delle leggi sull'ordinamento degli enti locali); il diritto di accesso in materia ambientale, disciplinato dal d.lgs. 10 agosto 2005, n. 195; l'accesso in materia di contratti pubblici, regolato dal d.lgs. 36/2023 ("Codice dei contratti pubblici"). E ancora l'accesso incidentale, l'accesso previsto dal codice dei dati personali, l'accesso nelle indagini difensive; l'accesso nei confronti delle imprese assicuratrici. Si veda: Lipari 2019. Si veda altresì: Cicatiello et al. 2022.

Sul punto, tra l'altro, il dibattito scientifico ha prospettato che, col tempo, alcune istanze conoscitive sarebbero destinate a divenire superflue[2].

2. Il principio di trasparenza nell'ordinamento giuridico italiano

Il diritto di accesso civico generalizzato contribuisce a consolidare le garanzie di trasparenza dell'azione amministrativa, dal momento che chiunque può accedere «ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione».

La trasparenza amministrativa è un principio regolatore dell'attività e dell'organizzazione della pubblica amministrazione, in base al quale essa è tenuta ad assicurare la visibilità, la conoscibilità e la decifrabilità delle modalità attraverso le quali opera nel perseguimento dell'interesse pubblico. Nell'accezione legislativa, come è noto, «la trasparenza è intesa come accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche»[3].

Più specificamente il concetto di trasparenza è stato ampliato dall'art. 2 del d.lgs. 25 maggio 2016, n. 97. Se, nella prima formulazione dell'art. 1 del d.lgs. 33/2013, il diritto di accesso è limitato alle «informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni», la formulazione vigente lo estende alla conoscenza di «dati e documenti detenuti dalle pubbliche amministrazioni».

Così come recita l'art. 1 del d.lgs. 97/2016 la trasparenza è il mezzo per garantire l'effettività dei principi di rilevanza costituzionale quali, l'eguaglianza, il buon andamento, la responsabilità, l'efficacia e l'efficienza nell'utilizzo delle risorse pubbliche, nonché l'integrità e la lealtà nel servizio alla nazione. Tuttavia, seppur elevata a "principio generale" dell'azione amministrativa, ha natura ancillare rispetto ai menzionati principi costituzionali e non trova nella Costituzione un riferimento autonomo.

Si noti che, durante i lavori dell'Assemblea Costituente si era ipotizzata la necessità di ancorare al testo costituzionale il «controllo popolare sulle pubbliche amministrazioni»; questa formula richiama le attuali «forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche», riconosciute dal legislatore ai consociati per mezzo degli istituti della trasparenza.

Gli onorevoli La Rocca e Togliatti avevano proposto un comma aggiuntivo nel corpo dell'art. 91 Cost., che corrisponde all'attuale art. 97 della Costituzione: «La legge determina i modi e le forme in cui si esercita il controllo popolare sulle pubbliche amministrazioni». L'emendamento proposto era «basato su un concetto universalmente accolto»: l'esercizio di un controllo sulla pubblica amministrazione da parte della «fonte, la sorgente della sovranità, del potere»[4]. L'emendamento fu respinto, in quanto ritenuto superfluo. Tale scelta costrinse nei decenni successivi il legislatore e la giurisprudenza costituzionale a offrire una lettura orientata del diritto dei consociati a controllare la pubblica amministrazione e a partecipare allo svolgimento dell'attività amministrativa[5].

Più specificamente, la giurisprudenza costituzionale – prima dell'emanazione della normativa sulla trasparenza – ha offerto diverse letture del principio in esame.

Una prima interpretazione lo qualifica come strumento idoneo a garantire la credibilità della pubblica l'amministrazione, affermando che le esigenze di trasparenza e di credibilità sono direttamente connesse al principio costituzionale di buon andamento degli uffici[6].

2. Sul punto si rimanda a Savino 2016; per l'analisi critica del rapporto tra diritto di accesso documentale e diritto di accesso civico generalizzato si veda: Moliterni 2019, p. 581 ss.
3. Foà 2017, p. 65. Si vedano inoltre: Carloni 2009; Carloni 2022; Villata 1987.
4. Seduta del 24 ottobre 1947, onorevole La Rocca.
5. Sul punto degno di menzione è il riferimento alla nota formula di "incoscienza costituzionale" si veda Calamandrei 1996, p. 123 ss.
6. Corte Cost., sentenza 4 maggio 2005 n. 172; Corte Cost., sentenza 22 aprile 2002 n. 145; Corte Cost., sentenza 3 giugno 1999 n. 206

Una seconda lettura, riferita al principio di pubblicità dell'azione amministrativa, ne sottolinea la funzione subalterna rispetto all'imparzialità e al buon andamento e lo ascrive a principio del patrimonio costituzionale comune dei Paesi membri dell'Ue, riconducibile all'obbligo di motivazione degli atti dell'Unione[7]. Un'altra lettura invece è più incline a ricondurlo al principio di efficienza dell'amministrazione pubblica, che si esplica attraverso un organizzazione razionale e un corretto funzionamento degli uffici[8].

Il legislatore italiano ha operato una sintesi tra queste interpretazioni: il principio di trasparenza funge così da collante tra il principio di legalità e il principio di efficienza della pubblica amministrazione[9].

Costituisce pertanto il mezzo per superare la tensione tra efficienza e legalità ergendosi a misura della legittimità e al contempo della "bontà" dell'azione amministrativa; ciò sul presupposto che l'attività della pubblica amministrazione assuma la configurazione di un "servizio" reso alla comunità nazionale in forza della lettura dell'art. 98 Cost.

In questo senso, la trasparenza è al tempo stesso mezzo e fine dell'azione amministrativa: strumento per garantire i diritti dei consociati e opportunità di integrazione tra il principio di legalità e il principio di efficienza. Tale risultato può essere pienamente raggiunto solo qualora il legislatore valorizzi la trasparenza, non limitata al controllo *ex post*, sugli esiti dell'azione amministrativa, ma si spinga ad incentivarla *ex ante*, come strumento di partecipazione dei cittadini per la definizione delle scelte incidenti sulla collettività[10].

Più specificamente, l'accessibilità totale a dati e documenti detenuti dalla pubblica amministrazione si qualifica in termini *promozionali* alla partecipazione. Come prescrive l'art 1 del d.lgs. 25 maggio 2016, n. 97 la trasparenza è intesa come accessibilità totale dei dati e dei documenti detenuti dalle pubbliche amministrazioni «allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche».

Come è noto, la partecipazione ha a che fare con la concreta possibilità per il cittadino di incidere sul governo e sull'amministrazione della cosa pubblica[11].

La promozione della partecipazione è un'espressione già utilizzata dal legislatore degli anni Settanta, con la legge dell'8 aprile 1976, n. 278 art. 1, espressamente finalizzata a «promuovere la partecipazione popolare alla gestione amministrativa delle comunità locali».

Più precisamente, veniva offerto un quadro normativo delle numerose esperienze che, in quegli anni, erano maturate all'interno di molti Comuni attraverso «l'istituzione dei c.d. consigli di quartiere e con il riconoscimento, in diverse forme, di strutture spontaneistiche sorte nelle diverse città»[12].

Tuttavia, la suddetta legge, priva di una reale portata innovativa, non agevolò concretamente «la partecipazione popolare sotto nessun profilo»[13], considerato anche che le strutture organizzative e gli strumenti di democrazia diretta previsti erano difficili da utilizzare.

A tal punto, risulta utile riflettere sull'elaborazione del concetto di partecipazione da parte del sistema giuridico[14].

La partecipazione, come è noto, ha una duplice valenza; se da un lato è «un valore in sé, in quanto rappresenta un'apertura in senso democratico dell'ordinamento», dall'altro è «un

7. Corte Cost., sentenza 17 marzo 2006 n. 104, punto 3.2; sentenza Corte di Giustizia dell'Unione europea, 2 aprile 1998 in causa C-367/95.
8. Corte Cost., sentenza 23 marzo 2007, n. 104, punto 2.9.
9. Si veda Ursi 2016.
10. Foà 2017, p. 66.
11. Gorgerino 2022, p. 99.
12. Casetta 1977.
13. *Ivi*, p. 67.
14. Oltre a: Levi 1977, si faccia riferimento a: Cassese 2007; Allegretti 2009.

concetto funzionale» ai vari contesti in cui trova riconoscimento[15].

Per comprendere la portata innovativa dell'accesso civico generalizzato è necessario riflettere sul rapporto tra accesso e partecipazione. Come si è già detto, l'ordinamento italiano declina l'accesso generalizzato, in termini di promozione del dibattito pubblico informato e di controllo diffuso sull'azione amministrativa, anche se «neppure la disposizione normativa sull'accesso generalizzato permette di ricavare i caratteri e le concrete modalità della partecipazione»[16].

Considerato che l'amministrazione della cosa pubblica coinvolge una pluralità di interessi e produce, pertanto, una spiccata conflittualità tra cittadini, amministrazioni e operatori economici privati, l'accesso civico generalizzato funge da valvola di controllo sull'attività amministrativa, più specificamente sul perseguimento delle funzioni istituzionali e sull'impiego delle risorse pubbliche.

Ad esso può attribuirsi una "rilevanza procedurale" tesa a favorire la trasparenza dei procedimenti decisionali della PA e, dunque, ad accrescere il consenso dei destinatari sull'attività amministrativa[17].

In controluce, si sa, ogni aspetto della attività amministrativa rimanda al rapporto tra rappresentanti e rappresentati. Da tale considerazione rileva l'attualità di un famoso dibattito sviluppatosi alla fine degli anni Settanta. Esso ruotava attorno all'idea che la spinta alla partecipazione emergesse nei periodi di crisi del sistema politico, «in situazioni di contrasto tra rappresentanti e rappresentati che dal terreno delle organizzazioni politiche in senso stretto si allarga a tutto l'organismo statale, originando tensioni e contrasti che manifestano l'inefficacia e l'incapacità di espansione e di persuasione dei gruppi dominanti»[18].

2.1. L'evoluzione normativa del diritto di accesso ai documenti amministrativi

In Italia l'istituto ispirato al *Freedom of Information Act* è stato introdotto in applicazione della disciplina normativa di prevenzione della corruzione[19].

Dal 23 dicembre 2016 chiunque può accedere a qualsiasi informazione in possesso delle pubbliche amministrazioni italiane, se non vi osta uno degli interessi pubblici o privati espressamente indicati dalla legge. L'accesso civico generalizzato interviene in via sussidiaria e ulteriore rispetto al tentativo della trasparenza imposto dal legislatore mediante crescenti obblighi di pubblicazione. Sul punto, la Corte Costituzionale ha sottolineato che le informazioni soggette a tali obblighi non sono selezionate in base al perseguimento di obiettivi legittimi. Da qui il rischio di generare "opacità per confusione"[20].

Il FOIA estende l'area del conoscibile oltre i confini stabiliti dagli obblighi di pubblicazione[21].

Precedentemente alla sua adozione, la legge generale sul procedimento amministrativo conferiva effettività al principio di trasparenza, ma non appagava la dimensione collettiva della partecipazione.

Gli accessi civici invece, accordando l'accessibilità alle informazioni a "chiunque", allargano le maglie del diritto dell'informazione.

Sul punto, si sottolinea che «il superamento del diritto di accesso previsto nella legge sul procedimento amministrativo è funzionale a valorizzare il principio di trasparenza in funzione democratica, sì da consentire ai cittadini un controllo diffuso sull'attività dei pubblici poteri, superando la diffidenza del ceto politico-amministrativo verso la verificabilità e contestabilità delle decisioni assunte»[22].

15. Chiti 1977, p. 39.
16. Cfr. Cauduro 2017, p. 604.
17. Il modello della partecipazione ambientale «costituisce un paradigma generale per la partecipazione ai piani e programmi con effetti sull'ambiente» Sul tema si rimanda a: Cocconi 2010, p. 139.
18. Chiti 1977, p. 85. Sul più ampio tema della crisi della rappresentanza si rinvia a Luciani 2001, p. 109 ss.
19. Si veda la Relazione illustrativa al d.lgs 25 maggio 2016, n. 97 e del d.lgs. 14 marzo 2013, n. 33.
20. In merito agli obblighi di pubblicazione si veda la pronuncia della Corte Costituzionale n. 20/2019 punto 5.3.1.
21. Cfr. Savino 2016.
22. Foà 2017, p. 67.

Del resto l'ordinamento italiano necessitava di adottare misure "severe e drastiche" per effetto dei moniti provenienti da organizzazioni internazionali (ONU, GRECO, OCSE) e dalla stessa Unione europea: le classifiche redatte dall'organizzazione *Transparency International* collocano ancora l'Italia tra i paesi in cui è più elevata la percezione della corruzione, strettamente legata ad una carenza di trasparenza.

L'originaria scelta del legislatore italiano sulla trasparenza è stata timida: inizialmente è stato riconosciuto, in capo alle pubbliche amministrazioni, un dovere di pubblicare le informazioni ritenute più rilevanti (c.d. *proactive disclosure*), successivamente è stato regolato il diritto del singolo di esigere dalle amministrazioni qualsiasi tipo di informazione non riservata (c.d. *reactive disclosure*).

La scelta di una *proactive disclosure* è riconducibile alla crisi della finanza pubblica: gli obblighi di pubblicazione attuabili a costo zero erano preferibili a un FOIA inevitabilmente oneroso, che avrebbe costretto le amministrazioni ad arginare le problematiche connesse all'ampliamento sia dei soggetti legittimati sia dell'oggetto della pretesa conoscitiva.

Tuttavia, gli insoddisfacenti risultati dell'accesso civico hanno ispirato la riforma, in vista di una disciplina che, «fermi restando gli obblighi di pubblicazione», si fondi sul «riconoscimento della libertà di informazione attraverso il diritto d'accesso […] di chiunque […] ai dati e ai documenti detenuti dalle pubbliche amministrazioni, […] nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati», così come sancito dall'art. 7, comma 1, lett. h), l. 7 agosto 2015, n. 124.

La libertà di informazione, a cui fa espresso riferimento la norma citata, è un aspetto della libertà di espressione, condizione essenziale per la democraticità dello Stato.

Più specificamente, l'informazione costituisce "l'architrave" dello Stato democratico, ragione per cui è necessario che gli amministrati siano posti nella condizione di acquisire conoscenze sui meccanismi di gestione del potere. D'altronde, solo in presenza di informazioni diffuse i cittadini possono maturare consapevolmente le proprie convinzioni e orientarle verso scelte consapevoli. In altre parole «la democrazia è scelta e, per scegliere, per decidere è necessario conoscere»[23].

Il tema della libertà di informazione, intesa nella duplice accezione di libertà di informare ed essere informati, è da tempo al centro dell'interesse della dottrina e della giurisprudenza.

Del resto, è stato sottolineato che l'art. 21 della Costituzione, avendo ad oggetto il profilo attivo della libertà d'espressione, lascia agli interpreti il compito di individuare misura e limiti del diritto passivo di essere informati[24].

In particolare il Consiglio di Stato con la sentenza 12 agosto 2016 n. 3631 fa chiarezza sul rapporto tra libertà di informazione e diritto di accesso. I giudici di Palazzo Spada rilevano che: «non si ravvisa nel corpo dello stesso art. 21 Cost., il fondamento di un generale diritto di accesso alle fonti notiziali, al di là del concreto regime normativo che, di volta in volta e nell'equilibrio dei molteplici e talvolta non conciliabili interessi in gioco, regolano tal accesso. In altre parole, occorre evitare ogni generalizzazione sul rapporto tra diritto d'accesso e libertà di informare. Il nesso di strumentalità tra le due figure, che pure esiste, si sostanzia non già reputando, […] il diritto di accesso qual presupposto necessario della libertà d'informare, ma nel suo esatto opposto. È il riconoscimento giuridico di questa che, in base alla concreta regolazione del primo, diviene il presupposto di fatto affinché si realizzi la libertà d'informarsi»[25].

Il concreto inverarsi della libertà di informazione passa pertanto attraverso il riconoscimento del diritto di accesso ai documenti e alle informazioni detenute dalla pubblica amministrazione.

Ne ripercorriamo le principali tappe evolutive.

In primo luogo, dal testo originario della l. 7 agosto 1990, n. 241, precisamente all'art. 22, si evinceva un nesso stringente tra trasparenza, imparzialità e accesso agli atti. «Al fine di assicurare la trasparenza dell'attività amministrativa e di favorirne lo svolgimento imparziale», si riconosceva un diritto

23. Sandulli-Droghini 2020, p. 4. Sulla giuridificazione dell'informazione si veda: Zeno-Zencovich 2009.

24. Gardini 2013, p. 879; Loiodice 1969; Arena 1979.

25. Consiglio di Stato, sez. IV, sentenza 12 agosto 2016 n. 3631; in tema di libertà di informazione si rinvia altresì a: Corte Cost. sent. 84/1969; Corte Cost. sent. 112/93; Corte Cost. 206/2019.

di accesso ampio a «chiunque vi abbia interesse per la tutela di situazioni giuridicamente rilevanti». Successivamente la legge 11 febbraio 2005 ha modificato la l. 241/1990 in senso restrittivo.

Viene meno il riferimento all'accesso come strumento di trasparenza e gli interessati (originariamente identificati come «chiunque vi abbia interesse per la tutela di situazioni giuridicamente rilevanti») vengono individuati nei «soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, che abbiano un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso».

Come è stato sottolineato, l'accesso diviene «strumento per acquisire una più completa rappresentazione della situazione di fatto e di diritto finalizzata alla tutela di una posizione giuridica qualificata»[26].

Solo con il d.lgs. 27 ottobre 2009, n. 150 (c.d. decreto Brunetta) la trasparenza viene declinata come «[…] accessibilità totale, [anche] attraverso lo strumento della pubblicazione sui siti istituzionali delle amministrazioni pubbliche, delle informazioni», con la dichiarata finalità di «[…] favorire forme diffuse di controllo del rispetto dei principi di buon andamento e imparzialità»[27].

Viene così riconosciuto in capo a ciascun cittadino il diritto di ottenere le informazioni pubbliche, con l'obiettivo dichiarato di favorire quel controllo generalizzato sull'operato delle pubbliche amministrazioni, che resta invece espressamente escluso dalla previsione *ex* art. 24, co. 3 della l. 241/1990.

Dall'analisi del decreto Brunetta emerge la duplice finalità della trasparenza. Essa se, da un lato, è finalizzata a garantire l'efficienza della pubblica amministrazione, attraverso la visibilità delle performance dell'amministrazione e dei servizi pubblici, dall'altro, mira a prevenire la corruzione, attraverso il controllo e la partecipazione ai procedimenti e agli assetti organizzativi[28].

Su questa seconda linea direttrice si colloca il successivo d.lgs. 14 marzo 2013, n. 33 che ha come obiettivo – in base alla legge delega 190/2012 – di prevenire e reprimere l'illegalità nella pubblica amministrazione. A tale scopo, già nella sua versione originaria, il d.lgs. 33/2013 identifica espressamente la "trasparenza pubblica" come «una finalità di rilevante interesse pubblico nel rispetto della disciplina in materia di protezione dei dati personali»[29].

Come già affermato, con tale atto normativo, oggetto della trasparenza non sono più il procedimento, il provvedimento ed i documenti amministrativi, ma le "informazioni" relative all'organizzazione, alla gestione e all'utilizzo delle risorse finanziarie, strumentali ed umane.

Si precisa che nella versione originaria del decreto, le pubbliche amministrazioni sono tenute ad adempiere agli obblighi sulla trasparenza, attraverso l'uso del "sito istituzionale" di ogni singola amministrazione, sul quale ogni utente potrebbe ricercare tutte le informazioni inerenti all'attività e all'organizzazione degli enti, senza la necessità di autenticarsi o essere in qualche modo identificato.

L'art. 9, co. 1, del d.lgs. 33/2013 prescrive che le informazioni oggetto dell'obbligo di pubblicazione devono essere rese disponibili sulla home page dei siti istituzionali, all'interno della sezione "Amministrazione trasparente", garantendone "la qualità" e assicurandone «l'integrità, il costante aggiornamento, la completezza, la tempestività, la semplicità di consultazione, la comprensibilità, l'omogeneità, la facile accessibilità» (art. 6, comma 1 del d.lgs. 33/2013).

Gli obblighi di pubblicazione previsti sono corredati da un consistente apparato sanzionatorio.

Il capo VI del d.lgs. 33/2013 prevede sanzioni dirette al responsabile della trasparenza, ai

26. Galetta 2016, p. 1043.

27. Così art. 11 co. 1 del d.lgs 150/2009.

28. Galetta 2016, p. 1045; si veda altresì: Sisto 2021. In particolare sul rapporto tra trasparenza e costi della politica: Allegri 2014.

29. Tale previsione, originariamente contenuta nell'art. 4 (comma 2), rubricato "Limiti alla trasparenza" è stata ora trasferita all'art. 7-*bis*, rubricato "Limiti alla pubblicazione", al comma 2. Il nuovo art. 5-*bis*, comma 2, statuisce tuttavia espressamente, alla lettera a), che «la protezione dei dati personali, in conformità con la disciplina legislativa in materia» è un possibile limite anche all'accesso civico.

dirigenti e agli organi politici che devono fornire i dati per realizzare la pubblicazione.

Oltre alle sanzioni a carico dei soggetti, sono previste anche sanzioni sull'atto, che bloccano l'efficacia del provvedimento[30]. Una sanzione particolare consiste poi nel c.d. accesso civico, previsto dall'art. 5 dell'originario d.lgs. 33/2013. Nella sua versione iniziale, infatti, l'accesso civico è identificato nell'obbligo, previsto in capo alle pubbliche amministrazioni, di pubblicare documenti, informazioni o dati, da cui discende «il diritto di chiunque di richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione».

Ai sensi della normativa vigente, l'accesso civico si realizza sia attraverso l'ostensione di dati e documenti, sia tramite «la pubblicazione di documenti, informazioni e dati concernenti l'organizzazione e l'attività delle pubbliche amministrazioni e le modalità per la loro realizzazione» (art. 1 d.lgs. 25 maggio 2016 n. 97).

Attraverso l'accesso civico in senso proprio, chiunque ha diritto di richiedere documenti informazioni o dati che l'amministrazione abbia omesso di pubblicare pur avendone l'obbligo.

L'accesso civico generalizzato invece prescinde dalla sussistenza di uno specifico obbligo di pubblicazione gravante sulla pubblica amministrazione.

Tale istituto è stato introdotto dal primo decreto legislativo attuativo della l. 124/2015, il d.lgs. 97/2016, con cui il Governo ha provveduto a modificare in modo sostanziale il d.lgs. 33/2013[31].

Con il suddetto decreto si ridefiniscono le modalità di attuazione del principio di trasparenza, ricondotto dal d.lgs. 33/2013 a ''finalità di rilevante interesse pubblico".

A tale scopo viene modificato l'oggetto della disciplina: nella versione precedente del decreto esso coincideva con gli «obblighi di trasparenza concernenti l'organizzazione e l'attività delle pubbliche amministrazioni», ora – in base al nuovo art. 2 co. 1 – corrisponde alla «libertà di accesso di chiunque ai dati e ai documenti detenuti dalle pubbliche amministrazioni e dagli altri soggetti di cui all'articolo 2-*bis*, garantita, nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati giuridicamente rilevanti […]».

Si tratta di una modifica assai rilevante, perché mette chiaramente in evidenza come lo scopo della normativa in materia di trasparenza non sia più, *in primis*, quello di ottenere la pubblicazione di documenti amministrativi, ma quello di garantire la libertà di accesso a dati e documenti in possesso della pubblica amministrazione «tramite la pubblicazione di documenti, informazioni e dati»[32].

Pertanto, la natura stessa dell'accesso civico subisce un cambiamento: da mera sanzione rispetto alla violazione dell'obbligo di pubblicare documenti, informazioni o dati, diventa un autonomo diritto (diritto di accesso civico) e lo strumento principale per la realizzazione del principio di trasparenza[33].

2.2. Il FOIA italiano: ambito soggettivo di applicazione e oggetto della disciplina

L'art. 2 co. 1 del d.lgs. 33/2013 sancisce che l'accesso civico spetta a "chiunque". Non si tratta, cioè, di un accesso riservato ai soli cittadini italiani.

Quanto invece ai soggetti passivi dell'accesso civico, il d.lgs. 97/2016 ha introdotto nel d.lgs. 33/2013 un nuovo art. 2-*bis*, rubricato "Ambito soggettivo di applicazione".

In particolare il diritto di accesso generalizzato può essere esercitato nei confronti di:

– tutte le amministrazioni pubbliche, come esemplificate all'art. 1, co. 2, del d.lgs. 30 marzo 2001, n. 165 e successive modificazioni, ivi comprese le autorità portuali, nonché le autorità

30. Cfr. art. 15, co. 2; art. 26, co. 3; art. 39, co. 3, del d.lgs. 33/2013.

31. Per un'analisi evolutiva della normativa in materia di accesso civico generalizzato si rinvia: Porporato 2017. Si veda inoltre il parere del Consiglio di Stato n. 515/2016.

32. Galetta 2016, p. 1048.

33. Recita il co. 2 dell'art. 5 che «Allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico, chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del presente decreto, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-*bis*».

amministrative indipendenti di garanzia, vigilanza e regolazione;
- gli enti pubblici economici e ordini professionali;
- le società in controllo pubblico come definite dal decreto legislativo emanato in attuazione dell'art. 18 della l. 7 agosto 2015, n. 124 (d.lgs. 19 agosto 2016, n. 175 c.d. "Testo unico in materia di società a partecipazione pubblica");
- le associazioni, fondazioni e enti di diritto privato comunque denominati, anche privi di personalità giuridica, con bilancio superiore a cinquecentomila euro, la cui attività sia finanziata in modo maggioritario per almeno due esercizi finanziari consecutivi nell'ultimo triennio da pubbliche amministrazioni e in cui la totalità dei titolari o dei componenti dell'organo d'amministrazione o di indirizzo sia designata da pubbliche amministrazioni.

Inoltre, il diritto di accesso generalizzato si applica, limitatamente ai dati e ai documenti inerenti all'attività di pubblico interesse disciplinata dal diritto nazionale o dell'Unione europea, anche:
- alle società in sola partecipazione pubblica come definite dal decreto legislativo emanato in attuazione dell'art. 18 l. 124/2015 (d.lgs. 175/2016);
- alle associazioni, alle fondazioni e agli enti di diritto privato, anche privi di personalità giuridica, con bilancio superiore a cinquecentomila euro, che esercitano funzioni amministrative, attività di produzione di beni e servizi a favore delle amministrazioni pubbliche o di gestione di servizi pubblici.

Nelle Linee guida adottate dall'ANAC il 28 dicembre 2016 n. 1309[34] è specificato come sia necessario comprendere il significato della disposizione legislativa che delimita il campo di applicazione dell'accesso civico generalizzato ai soggetti indicati al comma 3 dell'art. 2-*bis* del decreto trasparenza, «limitatamente ai dati e ai documenti inerenti all'attività di pubblico interesse disciplinata dal diritto nazionale o dell'Unione europea». La *ratio* della norma è quella «di garantire che la cura concreta di interessi della collettività, anche ove affidati a soggetti esterni all'apparato amministrativo vero e proprio, rispondano comunque a principi di imparzialità, del buon andamento e della trasparenza»[35].

Nel novero di tali attività si ritiene possano rientrare quelle qualificate come tali da una norma di legge, dagli atti costitutivi o dagli statuti delle società[36].

In merito alle amministrazioni di cui all'art. 1, co. 2 d.lgs. 165/2001, la norma si riferisce a: «tutte le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale».

L'elenco sintetico delle amministrazioni è stato pubblicato anche sulla Gazzetta Ufficiale – Serie Generale n. 226 del 28 settembre 2018, ai sensi dell'art. 1, comma 3 della l. 31 dicembre 2009, n. 196 e ss.mm. ("Legge di contabilità e di finanza pubblica")[37].

Per quanto attiene all'ambito soggettivo di applicazione dell'accesso civico generalizzato, un particolare problema interpretativo sorge in riferimento ai tribunali e alle Corti, istituzioni ricondotte nel novero delle "amministrazioni periferiche".

Sul punto, la circolare di dettaglio del Ministero della Giustizia n. 55828, emessa il 16 febbraio 2018, denominata "Linee guida operative concernenti le modalità di presentazione, trattazione e decisione delle richieste di accesso civico generalizzato", ha specificato che tra gli uffici dell'amministrazione periferica sono ricompresi gli uffici giudiziari di ogni stato e grado.

La complessità organizzativa degli uffici giudiziari è stata evidenziata nelle già citate Linee guida ANAC del 28 dicembre 2016.

34. ANAC 2016.
35. ANAC 2016, p. 9.
36. *Ibidem*.
37. L'elenco sintetico delle amministrazioni è stato pubblicato anche sulla Gazzetta Ufficiale – Serie Generale n. 226 del 28 settembre 2018, ai sensi dell'art. 1, comma 3 della l. 31 dicembre 2009, n. 196 e ss.mm.

In particolare, la determinazione n. 1309 precisa che l'accesso generalizzato riguarda atti, dati e informazioni, riconducibili a un'attività amministrativa, in senso oggettivo e funzionale. Esulano, pertanto, dall'accesso generalizzato «gli atti giudiziari, cioè gli atti processuali o quelli che siano espressione della funzione giurisdizionale, ancorché non immediatamente collegati a provvedimenti che siano espressione dello *ius dicere*, purché intimamente e strumentalmente connessi a questi ultimi»[38]. L'accesso e i limiti alla conoscenza degli atti giudiziari e di tutti gli atti che sono espressione della funzione giurisdizionale, anche se acquisiti in un procedimento amministrativo, sono infatti disciplinati da regole autonome previste dai rispettivi codici di rito. Si pensi alla speciale disciplina del segreto istruttorio, ai sensi dell'art. 329 c.p.p.; al divieto di pubblicazione di atti (art. 114 c.p.p.) e al rilascio di copia di atti del procedimento a chiunque vi abbia interesse, previa autorizzazione del pubblico ministero o del giudice che procede (art. 116 c.p.p.).

Nei giudizi civili, l'art. 76 disp. att. c.p.c., stabilisce che le parti e i loro difensori possono esaminare gli atti e i documenti inseriti nel fascicolo d'ufficio e in quelli delle altre parti e ottenere copia dal cancelliere; da ciò segue che l'accesso alle informazioni è consentito solo alle parti e ai loro difensori.

Specifiche previsioni sono poste dalla legge fallimentare che, nell'ambito delle procedure concorsuali, riconosce al comitato dei creditori e al fallito il diritto di prendere visione di ogni atto contenuto nel fascicolo; per gli altri creditori e i terzi invece l'accesso è consentito, purché gli stessi abbiano un interesse specifico e attuale, previa autorizzazione del giudice delegato, sentito il curatore.

Da quanto affermato fin ora, segue che la disciplina sull'accesso civico generalizzato riguarda anche dati, informazioni e documenti detenuti dagli uffici giudiziari, purché non si riferiscano ad un procedimento giurisdizionale, al quale invece si applicano le regole dettate dai codici di rito e dalle altre leggi speciali che disciplinano il processo[39].

L'accesso civico generalizzato – come già evidenziato – è esercitabile relativamente «ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione». Secondo le Linee guida dettate dall'Autorità Nazionale Anticorruzione n. 1309/2016 il "dato" intercetta un concetto informativo ampio, «da riferire al dato conoscitivo come tale, indipendentemente dal supporto fisico sui cui è incorporato e a prescindere dai vincoli derivanti dalle sue modalità di organizzazione e conservazione»[40]. Pertanto, la distinzione tra documenti e dati comporta che l'amministrazione sia tenuta a considerare come validamente formulate anche le richieste che si limitino a indicare i dati desiderati e non anche i documenti in cui essi sono contenuti. Non è comunque ammissibile una richiesta meramente esplorativa, finalizzata a scoprire di quali informazioni l'amministrazione dispone.

Le richieste inoltre non devono essere generiche, in quanto devono consentire l'individuazione del dato, del documento o dell'informazione, con riferimento, almeno, alla loro natura e al loro oggetto[41].

Se per "informazione" si intende la rielaborazione di dati detenuti dalle amministrazioni, contenuti in distinti documenti, è escluso che, per rispondere alla richiesta di accesso, l'amministrazione sia tenuta a formare o raccogliere o a procurarsi informazioni non in suo possesso. L'amministrazione

38. ANAC 2016, punto 7.6; Consiglio di Stato, sentenza 15 giugno 2021 n. 4644, in riferimento ad un'istanza di accesso civico generalizzato avente ad oggetto alcuni documenti inerenti a viadotti autostradali: «l'ostensione dei documenti non può riguardare gli atti acquisiti nell'ambito dei procedimenti penali o di procedimenti amministrativi di tipo ispettivo». L'accesso nel caso di specie è correttamente consentito solo con riferimento alla documentazione tecnica con precauzione di oscuramento volte a tutelare eventuali segreti industriali e commerciali.

39. Per quanto riguarda l'ostensione di atti acquisiti nei procedimenti penali si veda: Consiglio di Stato, sez. V, sentenza 15 gennaio 2021, n. 4644.

40. ANAC 2016, p. 9.

41. Cfr. Consiglio di Stato, parere n. 515/2016, par. 11.3; Consiglio di Stato, sez. VI, sentenza, 22 giugno 2020 n. 3981.

non ha dunque l'obbligo di rielaborare i dati ai fini dell'accesso generalizzato, ma solo a consentire l'accesso ai documenti nei quali siano contenute le informazioni già detenute e gestite dall'amministrazione stessa[42].

2.3. Eccezioni e limiti

La regola della generale accessibilità è temperata dalla previsione di eccezioni poste a tutela di interessi pubblici e privati, che possono subire un pregiudizio dalla diffusione generalizzata di talune informazioni.

Dalla lettura dell'art. 5-*bis*, co. 1, 2 e 3 del decreto trasparenza si possono distinguere due tipi di eccezioni, assolute o relative[43].

Il legislatore ha individuato un elenco di interessi per la protezione dei quali l'accesso è rifiutato se il diniego «è necessario per evitare un pregiudizio concreto»[44].

L'accesso generalizzato è escluso nei casi indicati al co. 3 dell'art. 5-*bis*, casi in cui, sulla base di una valutazione preventiva e generale, una norma di legge dispone la non ostensibilità di dati, documenti e informazioni o la consente secondo particolari condizioni, modalità e/o limiti, al fine di tutelare interessi prioritari e fondamentali.

Dette esclusioni definite altresì dal legislatore "eccezioni assolute", ricorrono:

a) in caso di segreto di Stato;
b) negli altri casi di divieto di accesso o divulgazione previsti dalla legge, ivi compresi i casi in cui l'accesso è subordinato dalla disciplina vigente al rispetto di specifiche modalità o limiti, inclusi quelli di cui all'art. 24, co. 1, l. 241/1990.

Esclusa la sussistenza dei limiti sopra elencati, possono ricorrere, invece, limiti (eccezioni relative o qualificate) posti a tutela di interessi pubblici e privati di particolare rilievo giuridico elencati ai commi 1 e 2 dell'art. 5-*bis* del decreto trasparenza.

Il legislatore non opera, come nel caso delle eccezioni assolute, una generale e preventiva individuazione di esclusioni all'accesso generalizzato, ma rinvia a una attività valutativa che deve essere effettuata dalle amministrazioni con la tecnica del bilanciamento, caso per caso, tra l'interesse pubblico alla *disclosure* generalizzata e la tutela di interessi giuridicamente rilevanti[45].

Più specificamente l'amministrazione è tenuta a verificare, una volta accertata l'assenza di eccezioni assolute, se l'ostensione degli atti possa determinare un pregiudizio concreto e probabile agli interessi indicati dal legislatore.

Sempre in riferimento alla valutazione delle istanze, il mancato riferimento normativo al "*public interest test*", avvicina invece il modello italiano ad altri ordinamenti come quello svedese (che sarà analizzato in seguito), in cui il potere dell'amministrazione si sostanzia nell'interpretazione di clausole generali, allo scopo di verificare se la concreta soddisfazione al diritto di informazione possa comportare un pregiudizio alla tutela degli interessi e finalità superindividuali tipizzate dalla norma.

L'accesso può essere rifiutato qualora il pregiudizio agli interessi indicati nei commi 1 e 2 sia concreto, ossia qualora sussista un preciso nesso di causalità tra l'accesso e il pregiudizio.

Come sottolineato dall'ANAC nelle Linee guida, l'amministrazione non può limitarsi a prefigurare il rischio di un pregiudizio in via generica e astratta, ma dovrà:

a) indicare chiaramente quale tra gli interessi elencati all'art. 5-*bis*, co. 1 e 2 viene pregiudicato;
b) valutare se il pregiudizio concreto prefigurato dipende direttamente dalla *disclosure* dell'informazione richiesta;

42. ANAC 2016, p. 10; sul punto si rinvia a Consiglio di Stato, sez. III, sentenza 16 febbraio 2021 n. 1426: «può essere respinta la richiesta di accesso civico generalizzato, nel caso in cui sia manifestamente onerosa o sproporzionata e comporti, quindi, un carico irragionevole di lavoro, tale da interferire con il buon andamento dell'Amministrazione»; TAR Umbria - Perugia, sez. I, sentenza 6 aprile 2021 n. 221; TAR Lazio - Roma, sez. III *quater*, sentenza 6 luglio 2022 n. 9258; TAR Lazio - Roma, Sez. III, sentenza 4 gennaio 2022, n. 25.
43. Sul tema dei limiti all'accesso civico generalizzato si segnala: Filice 2019.
44. Cfr. d.lgs. 14 marzo 2013, n. 33, art. 5-*bis*.
45. Sul punto si veda: Consiglio di Stato, sez. III, sentenza 10 febbraio 2022 n. 990; in tema di pregiudizio concreto e bilanciamento degli interessi coinvolti si veda: TAR Calabria - Catanzaro, Sez. II, 05/04/2022, n. 596; TAR Campania - Napoli, Sez. VI, 10/12/2019, n. 5837.

c) valutare se il pregiudizio conseguente alla *disclosure* è un evento altamente probabile, e non soltanto possibile[46].

Come premesso, la disciplina in esame prevede la possibilità di rigettare l'istanza di accesso civico generalizzato, qualora il diniego sia necessario per evitare un pregiudizio concreto alla tutela di uno degli interessi pubblici elencati nel nuovo art. 5-*bis*, co. 1 del d.lgs. n. 33/2013, inerenti a:

a) la sicurezza pubblica e l'ordine pubblico;
b) la sicurezza nazionale;
c) la difesa e le questioni militari;
d) le relazioni internazionali;
e) la politica e la stabilità finanziaria ed economica dello Stato;
f) la conduzione di indagini sui reati e il loro perseguimento;
g) il regolare svolgimento di attività ispettive.

L'art. 5-*bis*, co. 2, altresì sancisce che l'accesso generalizzato è rifiutato se il diniego è necessario per evitare il pregiudizio concreto alla tutela degli interessi privati specificamente indicati dalla norma:

a) la protezione dei dati personali;
b) la libertà e segretezza della corrispondenza;
c) gli interessi economici e commerciali di una persona fisica o giuridica, ivi compresi proprietà intellettuale, diritto d'autore e segreti commerciali.

2.4. Procedimento e forme di tutela

Per quanto attiene al procedimento, l'art. 5 co. 3 del d.lgs 33/2013 individua gli uffici a cui è possibile indirizzare l'istanza di accesso civico generalizzato. Essa può essere trasmessa per via telematica secondo le modalità previste dal decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni:

– all'ufficio che detiene i dati, le informazioni o i documenti;
– all'ufficio relazioni con il pubblico;
– ad un altro ufficio indicato dall'amministrazione nella sezione "Amministrazione trasparente" del sito istituzionale.

Si precisa che la pubblica amministrazione ha il potere di sindacare la finalità dell'istanza, verificando, in particolare, che la conoscenza delle informazioni richieste sia in linea con la *ratio legis* della norma.

Pertanto, la pubblica amministrazione può ritenere l'istanza di accesso civico meritevole di essere accolta, soltanto qualora «l'esigenza conoscitiva assuma una *rilevanza pubblica* e non anche quando essa resti confinata ad un bisogno esclusivamente *privato, individuale, egoistico o utilitaristico*»[47].

Da un punto di vista procedurale, l'istanza va comunicata d'ufficio a eventuali controinteressati; questi ultimi possono presentare una motivata opposizione all'accesso, entro dieci giorni dalla ricezione della comunicazione e, a tal fine, il termine per la decisione resta sospeso.

Il procedimento deve concludersi con provvedimento espresso e motivato, da adottare e comunicare al richiedente e agli eventuali controinteressati, nel termine di trenta giorni dalla presentazione dell'istanza.

In caso di accoglimento della richiesta, l'amministrazione trasmette tempestivamente al richiedente i dati o i documenti richiesti, ovvero, nel caso di omessa pubblicazione obbligatoria, li pubblica sul sito, comunicandolo al richiedente.

Nonostante l'opposizione dei controinteressati, l'amministrazione, salvi i casi di comprovata indifferibilità, trasmette al richiedente i dati o i documenti richiesti non prima di quindici giorni, decorrenti dalla ricezione della comunicazione ai controinteressati medesimi.

In caso di diniego parziale o totale all'accesso, ovvero in caso di mancata risposta allo scadere del termine per provvedere, il cittadino può attivare la speciale tutela amministrativa interna davanti al responsabile della prevenzione della corruzione e della trasparenza, formulando un'istanza di riesame, che dev'essere decisa, con provvedimento motivato, entro il termine di venti giorni.

In alternativa, per gli enti locali, può essere proposto ricorso al difensore civico, che si pronuncia entro trenta giorni dalla presentazione dello stesso. Se il difensore civico ritiene illegittimo il diniego o il differimento, lo comunica all'amministrazione e ne informa il richiedente. Se l'ente non conferma il diniego o il differimento entro trenta giorni

46. ANAC 2016, p. 11.
47. Cfr. circolare del Ministero della giustizia, 28 giugno 2018.

dal ricevimento della comunicazione del difensore civico, l'accesso è ritenuto assentito. Nel caso in cui l'accesso è negato o differito per la tutela di dati personali, il responsabile della prevenzione della corruzione e della trasparenza, ovvero il difensore civico, devono previamente sentire il Garante per la protezione dei dati personali, che si pronuncia nel termine di dieci giorni dalla richiesta.

Si precisa che la richiesta di riesame al responsabile della prevenzione della corruzione e della trasparenza e il ricorso al difensore civico possono essere presentati anche dal controinteressato, nel termine di quindici giorni dalla ricezione della comunicazione dell'avvenuto accoglimento della richiesta di accesso civico generalizzato (termine durante il quale l'atto di accoglimento, salvo non sia indifferibile, rimane inefficace).

Avverso la decisione dell'amministrazione o avverso quella del responsabile della prevenzione della corruzione e della trasparenza, il richiedente l'accesso può proporre ricorso al giudice amministrativo *ex* art. 116 c.p.a. ("rito in materia di accesso ai documenti amministrativi")[48].

Relativamente alla tutela giurisdizionale del controinteressato avverso il provvedimento di accoglimento dell'accesso civico generalizzato, nel silenzio dell'art. 5, deve ritenersi che essa spetti all'autorità giudiziaria ordinaria, ai sensi dell'art. 152 del d.lgs. 30 giugno 2003, n. 196 ("Codice in materia di protezione dei dati personali").

Occorre rilevare come il legislatore, a fini deflattivi ed acceleratori, abbia previsto un riesame "interno" (nei casi di diniego totale o parziale dell'accesso o di mancata risposta), a mezzo dell'intervento del responsabile della prevenzione della corruzione e della trasparenza[49].

Peraltro, tale riesame è alternativo rispetto al ricorso da proporre ad un altro soggetto indipendente, tenuto ad assicurare il rispetto delle leggi in ambito locale: il difensore civico[50].

Sul punto la circolare n. 2/2017, con cui il Dipartimento della funzione pubblica ha stabilito i criteri di "attuazione delle norme sull'accesso civico generalizzato, c.d. FOIA", evidenzia come la procedura di riesame «si discosta sia dalla norma che disciplina l'accesso ai documenti, che non prevede una procedura di tutela amministrativa interna, con la possibilità di chiedere il riesame a un altro soggetto appartenente alla stessa amministrazione, sia dalla disciplina in tema di obblighi di pubblicazione, per i quali è espressamente previsto dall'art. 5, co. 3, lett. d), che l'istanza vada inoltrata, già in prima battuta, direttamente al RPCT (*Responsabile della prevenzione della corruzione e della trasparenza*) e non, come per l'accesso generalizzato, all'ufficio che detiene i dati, o all'URP o ad altro ufficio indicato discrezionalmente dall'amministrazione sul sito istituzionale (art. 5, co. 3, lett. a), b) e c)»[51].

Si ritiene che la ragione giustificatrice di tale scelta poggi sulla considerazione che, contrariamente a quanto previsto dalla disciplina sull'accesso ai documenti, il silenzio dell'amministrazione sull'istanza di accesso civico "generalizzato", non dà luogo ad una fattispecie di silenzio significativo di segno negativo (silenzio-rigetto). L'art. 5 impone, infatti, l'obbligo per l'amministrazione di pronunciarsi con provvedimento espresso e motivato[52]. Da ciò segue che l'eventuale "silenzio" rappresenti una "mera inerzia", un'ipotesi, di silenzio-inadempimento, che obbliga il cittadino a rivolgersi al giudice amministrativo, attivando il rito di cui all'art. 117 c.p.a. (e successivamente, in caso di diniego espresso ai dati o documenti richiesti, il rito sull'accesso *ex* art. 116 c.p.a.)[53].

48. Intimando, a pena di inammissibilità del ricorso, anche gli eventuali controinteressati: TAR Lazio, Sez. I-*bis*, sentenza 29 gennaio 2017, n. 12788.

49. Cfr. Durante 2018.

50. Si precisa che nel caso di ricorso al difensore civico, il termine per il ricorso del richiedente *ex* art. 116 c.p.a. decorre dalla comunicazione della decisione di quest'ultimo (se negativa, ovviamente).

51. Circolare del Ministro della funzione pubblica 30 maggio 2017 n. 2, corsivo mio.

52. Consiglio di Stato sez. III, sentenza 2 febbraio 2022, n. 1482: «Il silenzio sull'istanza di accesso civico generalizzato non può essere qualificato come silenzio provvedimentale, in assenza di una espressa previsione di legge che attribuisca tale valore a quel contegno, come fa l'art. 25, comma 4, l. n. 241 del 1990 per l'istanza di accesso documentale».

53. Per un approfondimento della tesi in esame si rinvia a Durante 2018.

3. L'accesso agli atti nel diritto dell'Unione europea

Il legislatore italiano con l'adozione del d.lgs. 33/2013, come modificato dal d.lgs. 97/2016, si è mosso sulla scia dell'esplosione a livello globale delle legislazioni in materia di accesso ai documenti detenuti dai pubblici poteri, secondo il c.d. modello FOIA[54].

In base ai dati indicati dal progetto "*The Right to Information Rating*", fondato da *Access Info Europe* (AIE) e dal *Centre for Law and Democracy* (CLD), è stato rilevato che i Paesi dotati di una legge sulla libertà di accesso sono diventati da 13 nel 1990 a 128 nel 2020[55].

La diffusione del modello FOIA è stata sicuramente promossa dal diritto europeo e dalle convenzioni internazionali, come la Dichiarazione universale dei diritti dell'uomo del 1948 e la Convenzione europea dei diritti dell'uomo (CEDU), che riconoscono la libertà di informazione come diritto fondamentale.

Nell'ambito del diritto dell'Unione europea, il Trattato di Amsterdam del 1997 introduce l'art. 255 TCE, che espressamente riconosce il diritto di accedere ai documenti del Parlamento europeo, del Consiglio e della Commissione a qualsiasi cittadino dell'Unione e a qualsiasi persona fisica o giuridica residente o avente sede sociale in uno Stato membro.

L'art. 255 CE è stato poi riformulato con l'entrata in vigore del Trattato di Lisbona, che ha esteso il diritto di accesso ai documenti delle «istituzioni, organi o organismi dell'Unione e a prescindere dal loro supporto» (v. art. 15, co. 3 TFUE).

Ulteriori traguardi in materia sono: l'approvazione del regolamento 1049/2001/CE e l'inserimento degli artt. 41 e 42 nella Carta dei diritti fondamentali dell'Unione europea[56] (CDUE).

In riferimento ai suddetti articoli è necessario precisare che il diritto di accesso *ex* art. 42 CDUE deve essere tenuto distinto dal diritto di accesso previsto dal co. 2., lett. b) dell'art. 41 CDUE rubricato: "Diritto ad una buona amministrazione". Più specificamente l'ambito soggettivo di applicazione dell'art. 41 CDUE è più ampio di quello previsto dall'art. 42 CDUE, in quanto si riferisce ad "ogni persona" e non ai soli cittadini dell'Unione europea e alle persone fisiche e giuridiche che risiedano o abbiano la sede sociale in uno Stato membro. Oltre a ciò, la previsione contenuta nell'art. 41 CDUE si riferisce al più limitato «diritto di ogni persona di accedere al fascicolo che la riguarda».

Il diritto di accesso ai documenti delle istituzioni europee gode di un doppio statuto: quello di diritto fondamentale (*ex* art. 42 CDUE) e quello di principio generale dei Trattati (*ex* art. 15 TFUE)[57].

Se, da un lato, come affermato in precedenza, la diffusione del modello FOIA negli ordinamenti nazionali è stata promossa dal diritto europeo e dalla CEDU, deve riconoscersi, dall'altro, che il diritto europeo è stato considerevolmente influenzato dalle legislazioni degli Stati membri, soprattutto nord europei[58]. In altre parole, l'affermazione del diritto di accesso ai documenti pubblici europei si è realizzato attraverso un vero e proprio procedimento di osmosi tra i principi nazionali e il diritto comunitario[59].

Rilevato il nesso di fisiologica interconnessione tra l'ordinamento giuridico europeo e gli ordinamenti nazionali, è possibile ora delineare i tratti peculiari delle normative in materia di libertà di informazione, adottate da alcuni Paesi europei, quali la Svezia, la Francia, la Spagna.

54. Michel 2022.
55. Sulla moltiplicazione delle legislazioni in tema di libertà di informazione si veda: Mendel 2003; dato ripreso da Sandulli-Droghini 2020.
56. Ziller 2005, p. 538 ss; si rinvia inoltre a: Tommasi 2018. In tema di accesso agli atti dell'Unione europea si veda altresì: Rossi-Vinagre-Silva 2017.
57. Galetta 2016, p. 1038.
58. Chiti 2013, pp. 301-337.
59. Sul punto si veda: Tommasi 2018, p. 3. Per un'analisi evolutiva del diritto europeo in materia di accesso si rinvia a: Bifulco-Cartabia-Celotto 2001, p. 293 ss.; Alberti 2003, p. 63.

4. Applicazione del modello FOIA in Svezia

L'esperienza svedese in materia di accesso alle informazioni può essere elevata a vero e proprio modello di riferimento in materia di trasparenza[60].

Le norme sulla trasparenza e l'accesso libero agli atti della pubblica amministrazione sono contenute – sin dal 1766 – nella normativa svedese sulla libertà di stampa, che è parte stessa della Costituzione, il *Freedom of Press Act*.

La disciplina è stata poi aggiornata dall'adozione del *Public Access to Information and Secrecy Act*[61].

La legge sulla libertà di stampa prevede espressamente che, al fine di promuovere il libero scambio di opinioni e la disponibilità di informazioni chiare e precise, ogni cittadino svedese abbia il diritto di avere libero accesso ai documenti ufficiali, naturalmente con alcune eccezioni specificate nel *Secrecy Act*, il cui elenco ha tuttavia carattere tassativo e inderogabile.

Il sistema svedese riconosce una prevalenza assoluta al diritto dell'informazione: l'accesso ai documenti ufficiali delle pubbliche amministrazioni è permesso a chiunque.

I funzionari pubblici possono non solo rilasciare informazioni pubbliche quando sono richieste, ma anche divulgarle ai mezzi di comunicazione e stampa[62]. La *ratio* di tale scelta legislativa risiede, alla luce della storia costituzionale della Svezia, nel riconoscimento di un forte potere di controllo esercitabile da parte del cittadino nei confronti del potere politico.

Ma c'è di più: la peculiarità del modello FOIA svedese risiede proprio nel fatto che la trasparenza è intesa come «cessione di informazioni quali patrimonio della collettività» e non come rovesciamento del diritto alla segretezza[63].

Oggetto del diritto di accesso sono i documenti ufficiali delle pubbliche amministrazioni, ossia qualsiasi rappresentazione scritta, grafica o registrazione che possa essere letta, ascoltata, o comunque appresa anche con ausili tecnici.

La normativa si sofferma sulla definizione di *official document*: è ufficiale il documento che è detenuto da un'autorità pubblica e che è stato ricevuto o redatto da tale autorità.

Non sono considerati documenti ufficiali e, pertanto, sono esclusi dal diritto di accesso documenti quali memorandum, lettere o documenti preliminari o preparatori di atti pubblici.

Titolare del diritto di accesso è qualsiasi cittadino svedese o residente in Svezia, al quale è riconosciuto il libero accesso ai documenti ufficiali «in modo da incoraggiare il libero scambio di opinioni e la disponibilità di informazioni chiare e precise».

Considerato che la disciplina in materia non dà una definizione di pubblica autorità, devono considerarsi comunque tali: il *Riksdag* (Parlamento), il Governo, alcune società partecipate, fondazioni, associazioni, soggetti privati che esercitano poteri pubblicistici, le assemblee elettive statali, locali e le contee.

Ai sensi del Capo 2, articolo 2, del *Freedom of Information Act*, il diritto di accesso ai documenti ufficiali può essere limitato esclusivamente per legge e solo nei casi in cui la restrizione sia necessaria al fine di tutelare una serie di interessi prioritari, quali, ad esempio: la sicurezza del Regno e le relazioni con altri Stati; gli interessi fiscali e di politica monetaria, la prevenzione e la giustizia penale; gli interessi personali ed economici degli individui; la conservazione di specie animali o vegetali.

Il *Public Access to Information and Secrecy Act* comporta ulteriori restrizioni.

A tal riguardo, tale atto normativo indica tutti i casi in cui i documenti ufficiali sono coperti da segreto.

Per quanto attiene ai profili procedimentali, la richiesta di accesso a un documento ufficiale va presentata all'autorità che lo detiene, anche in forma anonima e senza necessità di motivazione.

Tuttavia, ai sensi del *Public Access to Information and Secrecy Act*, l'autorità può chiedere l'identificazione del richiedente e lo scopo della richiesta, al fine di valutare eventuali profili di riservatezza.

I documenti ufficiali debbono essere messi a disposizione dall'autorità al richiedente, immediatamente o in tempi brevi, nel luogo in cui si trovano

60. Cfr. Marchetti 2021.

61. L'atto è illustrato in un documento in lingua inglese redatto dal Ministero della Giustizia.

62. Cfr. Galetta 2016, p. 1033.

63. Sul punto si veda La Piscopìa 2016, p. 8.

(a meno che ciò sia impedito da gravi difficoltà) e gratuitamente. L'eventuale trascrizione o copia del documento può essere a pagamento.

L'autorità che rilascia l'atto potrebbe comunque imporre delle restrizioni in termini di pubblicazione o di utilizzo delle informazioni in esso contenute.

Il provvedimento espresso attraverso il quale un'autorità pubblica diversa dal *Riksdag* o dal Governo respinga una richiesta di esaminare un documento ufficiale o rilasci tale documento con riserva può essere impugnato. Qualora il documento da impugnare sia detenuto da un'autorità diversa da un Ministero, l'interessato può esperire un ricorso giurisdizionale. Se, invece, il provvedimento da impugnare è detenuto da un Ministero, si propone ricorso gerarchico al Governo.

Degna di menzione è altresì l'applicazione del principio di segretezza alle corti di giustizia.

In ambito giudiziario vige la regola secondo la quale le informazioni divulgate durante un'udienza pubblica sono generalmente considerate pubbliche, quelle invece afferenti ad un'udienza che si svolge in camera di consiglio non possono essere divulgate.

Si può pertanto affermare che le informazioni relative ad un giudizio o ad una decisione di un tribunale non siano coperte da segreto, a meno che il tribunale stesso, in casi eccezionali non disponga diversamente.

Il modello di trasparenza svedese, seppur emerge nell'ambito del contesto europeo per il carattere pionieristico, si pone come dissonante, per quanto attiene all'indubbia incompatibilità con il Regolamento (UE) 2016/679 sulla protezione dei dati personali: la garanzia del diritto di accesso ai documenti ufficiali è così ampia da penalizzare le opposte esigenze di riservatezza[64].

Sul punto e in un'ottica di comparazione, è necessario rilevare che a differenza del modello FOIA italiano, quello svedese non contempla la c.d. *proactive diclosure*, ossia l'obbligo di pubblicazione on line di documenti e dati in possesso delle pubbliche amministrazioni.

È invece ammessa la pubblicazione di dati estrapolati da documentazione pubblica e successivamente aggregati in banche dati, da parte di soggetti privati, che abbiano ottenuto un c.d. "certificato di pubblicazione" ai sensi dell'art. 9 cap. 1 della legge costituzionale sulla libertà di espressione.

La circostanza che il rilascio del relativo certificato sia *largely automatic* e che non siano state imposte restrizioni ai contenuti delle banche dati conduce alla possibilità che vengano pubblicati anche dati personali potenzialmente sensibili[65].

5. Applicazione del modello FOIA in Francia

Il *Code des relations entre le public et l'administration* (CRPA) ed in particolare il Libro III (*L'accès aux documents administratifs et la réutilisations des informations publiques*) e il Titolo I (*Le droit d'accès aux documents administratifs*) regolano la disciplina francese sull'accesso agli atti, che è stata introdotta con l'ordinanza n. 2015-1341 del 23 ottobre 2015, la quale ha di fatto sostituito la legge n. 78-753 del 17 luglio 1978, pur mantenendone le previsioni essenziali.

Ai sensi dell'articolo L300-2 del CRPA, sono considerati documenti amministrativi i documenti prodotti o ricevuti dalle autorità locali e da soggetti di diritto pubblico o da soggetti di diritto privato incaricati di un servizio pubblico, nell'ambito «de leur mission de service public».

Tali documenti includono registrazioni, relazioni, studi, verbali, statistiche, istruzioni, circolari, note ministeriali, corrispondenza, comunicazioni, previsioni, codici sorgente e decisioni.

Ai sensi dell'articolo L300-1 la legge garantisce ad ogni persona il diritto di accesso ai documenti amministrativi. Tuttavia, ai sensi dell'articolo L311-6, i documenti amministrativi possono essere comunicati solo alla persona interessata qualora la divulgazione:

– comprometta la protezione della vita privata, la riservatezza medica e il segreto commerciale, la segretezza del processo, le informazioni

64. Sul punto si veda la pronuncia della Corte europea dei diritti dell'uomo del 2 novembre 2010, caso *Gillberg v. Sweden*.

65. Per una riflessione sulla tutela delle istanze di riservatezza di veda: Österdahl 2016, p. 27 ss.; per un'analisi del modello svedese di accesso civico generalizzato si veda: Mattarella-Savino 2018.

economiche e finanziarie e le strategie commerciali o industriali[66];
- comporti un apprezzamento o un giudizio di valore su una persona fisica, identificata o facilmente identificabile;
- riveli il comportamento di una persona, dal momento che la divulgazione di tale comportamento potrebbe arrecarle un pregiudizio.

La normativa francese in materia di accesso ai documenti pubblici è soggetta a una serie di limitazioni; in particolare sono fatte salve una serie di eccezioni, così come sancito dall'art. L311-5.

Non possono formare oggetto di accesso (la versione originaria della norma utilizza il sostantivo *communication*) una serie di documenti, tra i quali: i pareri del Consiglio di Stato e dei tribunali amministrativi; i documenti della Corte dei conti di cui all'articolo L141-3 del *Code des juridictions financière*; i documenti redatti o detenuti dall'autorità Garante della concorrenza nell'esercizio delle sue competenze di indagine e decisione; i documenti redatti o detenuti dall'Autorità per la trasparenza della vita pubblica nel contesto delle assegnazioni di cui all'articolo 20 della legge n. 2013-907 dell'11 ottobre 2013 sulla trasparenza della vita pubblica.

Sono inoltre esclusi, dall'ambito oggettivo di applicazione della disciplina, i documenti amministrativi, la cui consultazione o comunicazione comprometterebbe:
- la segretezza delle deliberazioni del Governo e delle autorità responsabili del potere esecutivo;
- la difesa nazionale;
- il comportamento della politica estera della Francia;
- la sicurezza dello Stato, la sicurezza pubblica, la sicurezza delle persone o la sicurezza dei sistemi di informazione delle amministrazioni;
- la valuta e il credito pubblico;
- lo svolgimento di procedimenti giudiziari o le operazioni preliminari a tali procedimenti, salvo autorizzazione dell'autorità competente;
- la ricerca e prevenzione da parte dei servizi competenti di reati di qualsiasi tipo;
- i segreti protetti dalla legge, ai sensi dell'articolo L124-4 del Codice ambientale.

L'accesso ai documenti amministrativi è esercitato, su richiesta del richiedente e nei limiti delle possibilità tecniche dell'amministrazione (articolo L311-9), con costi che possono essere a carico del richiedente (articolo R311-11).

Sul punto è necessario sottolineare che il sistema francese non prevede una *proactive disclosure;* pertanto, in capo alle pubbliche amministrazioni non sono posti precisi obblighi di pubblicazione.

Per quanto riguarda l'iter procedimentale, se la pubblica amministrazione non si pronuncia entro un mese dalla richiesta di accesso, essa si intende rifiutata (articoli R311-12 e R311-13).

Qualsiasi provvedimento di diniego dell'accesso deve essere notificato al richiedente sotto forma di una decisione scritta motivata indicante i mezzi e i termini per il ricorso (articolo L311-14).

Ai sensi dell'articolo R343-1, entro due mesi dal rifiuto dell'accesso, l'interessato può esperire ricorso alla Commissione per l'accesso ai documenti amministrativi (*Commission d'accès aux documents administratifs* – CADA), un'autorità amministrativa indipendente incaricata di garantire la libertà di accesso ai documenti amministrativi e agli archivi pubblici e il riutilizzo dell'informazione pubblica[67]. Il procedimento si conclude con il rilascio, da parte della CADA, di un parere funzionale all'eventuale e successivo ricorso giurisdizionale, emesso entro un mese dalla richiesta dell'istante.

In mancanza del parere entro il termine stabilito, si applica l'istituto del silenzio-rigetto.

Sicuramente l'esperienza francese in materia di FOI suscita una serie di osservazioni.

La legge n. 78-753 ha definito già nel 1978 la *liberté d'acces aux documents administratifs* come *droit de toute personne à l'information*; tuttavia l'affermazione del diritto all'informazione non implica, nella prassi, una sua concreta applicazione.

66. Una specificazione è d'obbligo per le informazioni mediche che sono comunicate all'interessato, in base alla sua scelta, direttamente o tramite un medico da lui designato a tale scopo, in conformità con le disposizioni del codice L1111-7 di salute pubblica.

67. La CADA pubblica sul proprio sito un rapporto annuale di attività: e in conformità all'articolo L342-3 pubblica regolarmente l'elenco dei pareri favorevoli emessi dalla Commissione. Sulle funzioni della CADA si veda Picard 2013.

Più specificamente, il diritto di accedere liberamente alle informazioni contenute nei documenti amministrativi risente di alcuni nodi problematici della legislazione in materia.

Innanzitutto una limitazione attiene all'ambito di applicazione oggettivo della disciplina normativa che, come è stato già sottolineato in precedenza, è circoscritto per lo più al documento amministrativo formalizzato e definitivo.

Ulteriori criticità sono ravvisabili nei tempi troppo lunghi per il rilascio dei pareri da parte della CADA e nella rigida applicazione dell'istituto del silenzio-rifiuto, in caso di richiesta di accesso ai documenti amministrativi[68].

6. Applicazione del modello FOIA in Spagna

In Spagna il diritto di accesso è regolato dalla legge n. 19 del 9 dicembre 2013 *de transparencia, acceso a la información pública y buen gobierno*[69].

Ai sensi dell'art 12 tutte le persone hanno il diritto di accedere alle informazioni pubbliche, come previsto nell'articolo 105 (b) della Costituzione spagnola.

Le informazioni pubbliche sono intese come i contenuti o i documenti, che, indipendentemente dal formato o supporto, sono elaborati o acquisiti nell'esercizio delle loro funzioni (articolo 13) da uno dei soggetti previsti nell'ambito di applicazione del titolo I della legge in esame.

Più specificamente, l'art. 2 della legge n. 19 del 9 dicembre 2003 contiene un elenco di tutte le amministrazioni, le autorità indipendenti, gli organismi di diritto pubblico a cui essa è applicabile.

Tra di esse sono annoverate: *la Casa de su Majestad el Rey, el Congreso de los Diputados, el Senado, el Tribunal Constitucional y el Consejo General del Poder Judicial, así como el Banco de España, el Consejo de Estado, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo Económico y Social* (art. 2, comma 1 (f)).

Il diritto di accesso può essere limitato nei casi in cui accedere all'informazione implichi un danno:

- alla sicurezza nazionale;
- alla difesa;
- alle relazioni estere;
- alla sicurezza pubblica;
- alla prevenzione, indagine e sanzione di illeciti penali, amministrativi o disciplinari;
- all'eguaglianza delle parti nei processi giudiziari e alla tutela giurisdizionale effettiva;
- alle funzioni amministrative di vigilanza, ispezione e controllo;
- agli interessi economici e commerciali;
- alla politica economica e monetaria;
- al segreto professionale e alla proprietà intellettuale e industriale;
- alla garanzia della riservatezza o al segreto nei processi decisionali;
- alla tutela ambientale.

L'applicazione dei casi limite deve essere proporzionata a precise istanze di protezione, che hanno a che fare con le circostanze del caso concreto.

Se l'informazione richiesta contiene dati personali, ai quali si riferisce il paragrafo 2 dell'articolo 7 della *Ley Orgánica* 15/1999, l'accesso può essere autorizzato solo se vi è il consenso espresso dato per iscritto dall'interessato, a meno che quest'ultimo non avesse già reso pubblici i dati prima della relativa richiesta[70].

Quando l'informazione oggetto dell'istanza non contenga dati sensibili, l'organo al quale essa è diretta deve consentire l'accesso, previa ponderazione "sufficientemente ragionevole" dell'interesse pubblico alla divulgazione dell'informazione, dei diritti degli interessati e del diritto fondamentale alla protezione dei dati personali (art. 15, co. 3)[71].

Ai fini della realizzazione della ponderazione di cui sopra, la pubblica amministrazione dovrà tenere in considerazione i seguenti criteri:

68. Per approfondire la disciplina in materia di accesso ai documenti amministrativi nell'ordinamento giuridico francese si rinvia a: Dandelot 2018; Mattarella-Savino 2018; Ziller 2019.
69. La disciplina normativa oggetto della trattazione è consultabile sul sito del BOE. Per un'analisi del modello spagnolo di accesso civico generalizzato si faccia riferimento a: Mattarella-Savino 2018; Guichot Reina 2014; Gimeno Feliù 2014.
70. In tema di diritto di accesso alle informazioni e protezione dei dati personali si veda: Piñar Mañas 2015.
71. In tema di diritto di accesso alle informazioni e interpretazione giurisprudenziale si veda Rivas Martínez 2019.

a) il minor danno ai soggetti interessati derivante dalla decorrenza dei termini stabiliti dall'art. 57 della legge 16/1985, del 25 giugno, relativa al patrimonio storico spagnolo;
b) la motivazione dell'istanza da parte dei richiedenti, l'esercizio di un diritto o il fatto che essi siano ricercatori e giustificano l'accesso con motivi, storici scientifici o statistici;
c) il minor danno dei diritti dei soggetti interessati nel caso in cui i documenti contengano unicamente dati di carattere meramente identificativo degli stessi;
d) la maggior garanzia dei diritti dei soggetti interessati, nel caso in cui i dati contenuti nel documento possano interessare la loro intimità o la loro sicurezza o si riferiscano a minori di età.

Il c.d. *Public Interest Test* – il bilanciamento compiuto in concreto da parte della pubblica amministrazione tra l'interesse pubblico alla conoscibilità e "l'interesse limite" (pubblico o privato), individuato dal legislatore spagnolo – è previsto in maniera analoga dal Regolamento (CE) 1049/2001.

Come è noto, il succitato Regolamento europeo individua, da un lato, una serie di eccezioni assolute, per la cui applicazione vale esclusivamente il criterio del pregiudizio concreto a interessi ritenuti di rango superiore; dall'altro, una serie di eccezioni relative, per le quali, il criterio del pregiudizio concreto è mitigato dall'obbligo di bilanciamento con l'eventuale interesse pubblico prevalente alla divulgazione[72].

Sulla base di quanto finora esposto, la legislazione spagnola sul diritto di accesso alle informazioni costituisce un modello di riferimento sia per la completezza e la chiarezza sia per la conformità alla normativa europea in materia di accesso ai documenti delle istituzioni dell'Ue.

In riferimento al procedimento, l'esercizio del diritto di accesso ha inizio con la presentazione della domanda indirizzata al titolare dell'amministrazione o all'ufficio in possesso delle informazioni.

Il richiedente non è tenuto a motivare la sua richiesta di accesso. Può, tuttavia, indicarne i motivi, che possono essere presi in considerazione al momento della pronuncia (art. 17, co. 3).

La pronuncia favorevole o sfavorevole all'accesso deve essere notificata al richiedente e ai terzi interessati, entro il termine massimo di un mese dal ricevimento dell'istanza di accesso da parte dell'amministrazione competente a decidere.

L'accesso alle informazioni si realizza prevalentemente in via elettronica a meno che il soggetto richiedente non abbia espressamente segnalato un'altra modalità (art. 22, co. 1).

Quando non vi può essere accesso al momento della notifica della pronuncia, esso dovrà essere concesso, in qualsiasi caso, entro il termine di 10 giorni (art. 22, comma 2).

Eventuali reclami avverso la pronuncia di accesso possono essere presentati prima dell'impugnazione in via contenzioso-amministrativa, al *Consejo de Transparencia y Buen Gobierno*, entro un mese a decorrere dal giorno seguente alla notifica dell'atto impugnato o dal giorno successivo alla data in cui si verifichino gli effetti del silenzio assenso (art. 24, co. 1).

6.1. Cenni sulla trasparenza in ambito giudiziario

In ambito giudiziario il diritto di accesso è stato disciplinato dalla *Ley Orgánica* 6/1985 sul *Poder Judicial*[73].

Più specificamente l'articolo 234, comma 2 della legge sopra citata ha sancito che qualsiasi individuo che vanti un interesse diretto e legittimo ha il diritto a ottenere copie non certificate dei documenti che fanno parte del fascicolo, qualora essi non siano coperti da segreto, né riservati.

In riferimento al diritto di accesso alle sentenze e ad altri provvedimenti giurisdizionali, l'art. 235 *bis* della *Ley Orgánica* 6/1985 stabilisce che esso può essere concesso, solo previo oscuramento dei dati personali, nel pieno rispetto del diritto alla privacy, nonché nel rispetto dei diritti delle persone sottoposte a un particolare regime di protezione;

72. Sul tema si rinvia a: Corte di giustizia, 3 luglio 2014, causa C. 350/2012, *Consiglio dell'Unione europea c. Sophie in 't Veld*; Corte di giustizia, 17 ottobre 2013, causa C. 280/2011, *Consiglio dell'Unione europea c. Access Info Europe*, punto 31-32.
73. Per la consultazione della Ley Orgánica 6/1985, del 1° luglio, sul *Poder Judicial* si veda il testo pubblicato sul BOE. Sulla trasparenza amministrativa si rinvia a: Mir Puigpelat 2017; Guardiola 2018.

eventualmente nel rispetto dell'anonimato delle vittime e delle parti lese.

Degno di menzione è anche il "Piano della trasparenza giudiziaria"[74], deliberato dal Consiglio dei Ministri su proposta del Ministro della Giustizia il 28 ottobre 2005.

In tale atto normativo l'obiettivo di realizzare una giustizia trasparente si somma alla necessità per i cittadini di comprendere il linguaggio giudiziario; in tal senso significativo è il richiamo all'esposizione in maniera chiara dei termini delle notificazioni e delle citazioni.

Il Piano della trasparenza giudiziaria prevede altresì che siano resi disponibili gratuitamente i formulari, utili per l'esercizio dei diritti nei tribunali, quando non sia obbligatoria la presenza dell'avvocato e del procuratore.

L'art. 14 co. 1 della legge 15/2003 stabilisce che il Piano della trasparenza giudiziaria costituisce uno strumento fondamentale per le amministrazioni pubbliche e per il *Consejo General del Poder Judicial* per la pianificazione, lo sviluppo e l'esecuzione delle politiche pubbliche relative all'amministrazione della giustizia. Più specificamente, il Piano di Trasparenza sancisce per le parti e per ogni persona, che rivendichi un interesse legittimo, il diritto di conoscere il contenuto e lo stato dei processi in conformità con le disposizioni delle leggi processuali, attraverso l'accesso a documenti, libri, archivi e atti giudiziari non riservati.

Nel Titolo V inoltre è riportato un ricco e dettagliato elenco di informazioni utili, che ogni organo giudiziario è tenuto a rendere pubbliche, secondo i termini e le modalità definite dalla Commissione Nazionale per le statistiche giudiziarie. In particolare, si fa menzione del numero dei dipendenti, delle informazioni sul bilancio e sulle spese, dei contratti, delle statistiche sulla durata dei processi, dell'evoluzione dei carichi di lavoro, del numero e dell'età media dei giudici, dei pubblici ministeri, degli impiegati, degli avvocati, nonché dei compensi degli avvocati, degli esperti e dei medici forensi.

7. Il FOIA federale statunitense

Il *Freedom of Information Act* (FOIA) statunitense è da sempre considerato una pietra miliare nel percorso evolutivo dell'accesso a documenti e informazioni della pubblica amministrazione[75].

Il *Freedom of Information Act* si è sviluppato in un contesto giuridico-culturale in cui era forte l'istanza di riconoscimento di un diritto a manifestare liberamente il proprio pensiero attraverso la carta stampata; ciò, tra l'altro, sin dall'epoca in cui gli Stati Uniti d'America erano una colonia britannica. Si trattò, di rivendicare il diritto di contestare (per iscritto e di diffondere in tal modo le relative informazioni) «arbitrary political power, preparing the way for the revolutionary concepts of popular sovereignty and the people's right to know, which were eventually embodied in the American Constitution»[76].

Anche dopo la dichiarazione di indipendenza e l'adozione della Costituzione USA, la sua applicazione da parte delle Corti fu molto ampia. Dal 1925 nel caso *Gitlow v. New York*, la Corte Suprema si pronunciò a favore dell'applicabilità del Primo emendamento, che riconosce la libertà di parola e di stampa, anche agli Stati federati. Successivamente, in merito al caso *Grosjean v. American Press. Co.* la Corte fece riferimento alla lotta del popolo inglese «to establish and preserve the right […] to full information in respect of the doings or misdoings of their government»[77] e concluse affermando che proprio tale esperienza aveva condotto all'adozione del Primo Emendamento.

Il *Freedom of Information Act* fu adottato nel 1966 e nella sua versione originaria prevedeva che ogni persona avesse diritto di richiedere l'accesso ai "record" posseduti dalle agenzie federali, salvo che si trattasse di documenti o dati la cui divulgazione fosse esclusa in ragione di uno dei nove motivi di esclusione previsti dal FOIA o di una delle tre speciali clausole di esclusione previste in favore di FBI e forze di sicurezza federali. Non erano previsti né termini per rispondere alle richieste di accesso né sanzioni per il caso di violazione della relativa disciplina.

74. Il "Piano della trasparenza" è consultabile sul sito del BOE.

75. Interessante la comparazione tra l'esperienza giuridica statunitense e quella italiana, cfr. Lunardelli 2023.

76. Foerstel 1999, p. 8.

77. *Grosjean v. American Press Association*, 297 U. S. 233 (1936).

Nella prassi, pertanto, molte agenzie federali opponevano ritardi paralizzanti alle istanze di accesso. I richiedenti inoltre erano scoraggiati dal pagamento di importi elevati necessari per accedere al record. Si noti, come l'espressione record non faccia riferimento alle informazioni in quanto tali, ma al documento che le contiene.

Il *Freedom of Information Act* fu modificato dal *Openness Promotes Effectiveness in our National Government Act* nel 2007, dall'*Open FOIA Act* del 2009 e dall'emendamento *FOIA Improvement Act* del 2016[78].

Oggetto del FOIA federale statunitense sono tutti i documenti in possesso di un ente governativo federale, in qualsiasi formato, incluso il formato elettronico. Sono compresi anche i documenti di un ente governativo nella disponibilità di un soggetto terzo che li detiene per motivi di gestione archivistica. Esclusi dal diritto di accesso sono i documenti detenuti dal Congresso, dai tribunali e da parte dei Governi e delle agenzie governative dei singoli stati federati.

La legge suddivide gli atti pubblici in due categorie:

1) i documenti che devono essere pubblicati nel *Federal Register*, ed altri atti a carattere interno, quali ad esempio gli organigrammi o le istruzioni per lo staff a contatto con il pubblico;
2) i documenti non pubblicati, che devono essere resi disponibili a richiesta del pubblico.

Sono esclusi dall'obbligo di pubblicità e dal diritto di accesso le seguenti nove categorie di documenti: «1. classified information for national defence or foreign policy; 2. internal personnel rules and practices; 3. Information that exempt under other laws; 4. trade secrets and confidential business information; 5. inter-agency or intra-agency memoranda or letters that are protected by legal privileges; 6. personnel and medicaI files; 7. law enforcement records or information; 8. information conceming bank supervision; 9. geological and geophysical information».

Qualsiasi persona o organizzazione, indipendentemente dalla cittadinanza o dal paese di origine, è titolare del diritto di accesso ai documenti sopra specificati, che può essere esercitato nei confronti di qualsiasi *agency* federale; più precisamente, nei confronti di dipartimenti esecutivi o militari, enti governativi o controllati dal Governo, aziende attive nel ramo esecutivo del Governo (incluso l'Ufficio esecutivo del Presidente), autorità indipendenti.

Ai sensi del U.S.C. § 551, è espressamente escluso l'esercizio del diritto di accesso nei confronti:

- del Congresso;
- dei tribunali federali (courts);
- del Governo dei territori e dei possedimenti;
- del Governo del Distretto di Columbia.

La richiesta di accesso a un documento deve essere corredata da una descrizione del documento stesso e deve essere compilata in ottemperanza a regole procedurali predeterminate.

I documenti devono essere forniti nel formato richiesto, se disponibile.

Ogni ente pubblica le procedure relative al diritto di accesso e gli importi applicabili.

Le agenzie governative devono rispondere in 20 giorni lavorativi e sono tenuti a motivare la decisione.

È ammesso il ricorso gerarchico al direttore dell'ente governativo che ha rifiutato l'accesso, il quale ha l'obbligo di adottare una decisione nel termine di 20 giorni.

Se il diniego viene confermato, è previsto il ricorso giurisdizionale[79].

Il giudice può imporre all'ente governativo di rendere pubblici i documenti.

Come è noto, il modello FOIA statunitense è considerato come il modello di riferimento per valutare l'adeguatezza degli altri modelli[80].

78. Si precisa che il Freedom of Information Act è contenuto al paragrafo 552 del Codice delle leggi degli Stati Uniti; la versione italiana è consultabile sul sito del FOIA. Per l'analisi del FOIA statunitense alla luce delle modifiche legislative si rinvia a: Galetta 2016, pp. 1021-1032; per una lettura comparata dell'accesso civico italiano e di quello statunitense si rinvia a: La Piscopìa 2016.
79. In caso di ricorso giurisdizionale è competente a decidere la corte del distretto in cui il ricorrente risiede o dove svolge la propria attività o in cui si trova la documentazione, oppure il distretto di Columbia.
80. Sul modello FOIA americano si rinvia a: Ginsberg 2015; Cullier-Davis 2010.

Il modello italiano ha mutuato tre profili dal modello americano di FOIA: il "doppio binario" tra obblighi di pubblicazione e richieste di accesso civico; l'accessibilità – in linea di principio – totale ai documenti delle amministrazioni statali; il riconoscimento dell'accesso anche a chi non dimostri la titolarità di un interesse specifico alla conoscenza degli atti[81].

Tuttavia, come è stato sottolineato da attenta dottrina il livello di implementazione del FOIA a livello federale si è collocato, per lungo tempo, a livelli bassissimi[82].

Neppure la c.d. "*openness initiative*" promossa nel 1993, durante l'amministrazione Clinton, è stata in grado di apportare cambiamenti positivi alla criticità della situazione. Più nello specifico, con l'adozione dell'E-FOIA, in vigore dal 31 marzo 1997, le agenzie federali avrebbero dovuto rendere disponibili nelle *Reading Rooms*, tutti quei documenti che fossero già stati oggetto di richieste di accesso. Tale obbligo, decorrente dal 1 novembre 1997, avrebbe dovuto ridurre i ritardi cronici delle agenzie nell'evadere le richieste di accesso[83]. Tale soluzione legislativa non ha però permesso di porre un argine allo scarso livello di attuazione del FOIA da parte delle agenzie federali.

Le ragioni della scarsa applicazione del FOIA sono in parte sintetizzate in un'intervista del 1998 al FOIA Director del *Department of Health and Human Services*.

Nel tentare di spiegare le ragioni delle difficoltà di applicazione del FOIA nel Dipartimento da lui diretto, anche dopo l'approvazione del E-FOIA, egli osservava che: «Whatever they do to this statute and whatever they do to the hardware, they're never going to change the fact that freedom of information is a labor intensive activity. Even when you get the fancy hardware that allows you to scan in the record and then read it and redact it electronically, you still need somebody to run the blasted machine. And you need somebody who understands both the statute and the nature of the work that the organization is involved in»[84].

Da un'analisi più accurata della situazione risulta senza dubbio un atteggiamento di ostilità o quanto meno di scarso entusiasmo da parte delle agenzie governative nei confronti dell'idea di trasparenza e delle sue implicazioni; inoltre può affermarsi che i ritardi nelle risposte alle richieste di accesso ai sensi del FOIA sono inerenti alla natura stessa del lavoro richiesto per evaderle, a fronte dell'inadeguatezza del personale e dell'inadeguato finanziamento previsto per il compimento delle relative attività[85].

Un altro aspetto importante da tenere in considerazione è l'atteggiamento prevalente nelle corti statunitensi. Sul punto, è stato rilevato come, sin dal principio, le corti statunitensi abbiano offerto un sostegno assai timido all'applicazione del FOIA; ed abbiano al contrario mantenuto un atteggiamento di ampia riverenza nei confronti delle richieste del Governo e delle agenzie governative di mantenere il segreto su tutte quelle questioni che avrebbero potuto avere un nesso, anche molto indiretto, in particolare col tema della sicurezza nazionale[86].

81. Si veda Falletta 2016, p. 2.

82. Foerstel 1999, p. 163 ss.; Ratish 2007.

83. Galetta 2016, p. 1027.

84. Foerstel 1999, p. 85.

85. *Ivi*, p. 44. Sul punto emblematica è la dichiarazione fatta dal procuratore generale del Presidente Johnson, Ramesey Clark, durante un'intervista rilasciata a Foerstel: «I told the agencies to work hard at complying with the FOIA, but they were almost uniformly offended by the statute itself. They thought it implied that they weren't trusted and they feared that the FOIA would force them to work in a gold fish bowl, observed by the public».

86. A proposito di «interplay of overclassificalion and excessive judicial deference» si veda Nevelow Mart-Ginsburg 2014, p. 725 ss. Si rimanda altresì alla decisione della Corte Suprema USA del 1989, *Department of justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989), 764 (Foia's purpose decision) nella quale si fa riferimento alla necessità di avere chiaro quale è l'obiettivo centrale del FOIA nel decidere se consentire o meno l'accesso agli atti. A questa restrittiva interpretazione del FOIA si è ispirata gran parte della giurisprudenza almeno per tutto il decennio successivo. Per approfondimenti si veda in particolare: Halstuk-Chamberlin 2006, p. 511 ss. La questione della concreta applicazione della normativa in materia di trasparenza è trattata

Tale atteggiamento è stato facilitato grazie dall'ampia lista di deroghe all'applicazione del FOIA.

8. Considerazioni conclusive

La disamina fin ora svolta mette in luce il nucleo centrale comune delle legislazioni prese in esame.

La disponibilità delle informazioni che riguardano l'esercizio del potere pubblico ridisegna il rapporto intercorrente tra cittadino e autorità e decreta il passaggio da una democrazia puramente procedurale ad una forma di governo in cui assumono rilievo le precondizioni del processo democratico. In tale ottica, il diritto di essere informati e la trasparenza, intesa come principio e diritto, rappresentano precondizioni necessarie per l'esercizio della democrazia.

Il FOIA assicura ai cittadini un controllo diffuso sul corretto esercizio del potere da parte delle pubbliche amministrazioni; da ciò segue che la sua concreta applicazione è in grado di determinare il grado di sviluppo di un ordinamento democratico, la sua "qualità".

Ogni *Freedom of Information Act*, analizzato sia negli elementi strutturali che in quelli squisitamente procedurali, ha rivelato delle peculiarità.

I tratti differenziali delle singole esperienze oggetto di indagine vanno sicuramente decifrati nell'ambito del quadro sociale e culturale in cui il diritto di accesso alle informazioni si è sviluppato. A titolo esemplificativo, il FOIA statunitense, elevato molto spesso a modello di riferimento, nonostante gli esiti non proprio soddisfacenti in termini di effettività, si inserisce in un contesto culturale che ruota principalmente attorno al rapporto elettori-eletti e, solo in maniera marginale, al rapporto tra cittadino e pubblica amministrazione. In tale prospettiva, l'acquisizione delle informazioni deve essere letta in termini di possibilità per il cittadino di partecipare attivamente alla politica. Sul punto è necessario sottolineare che le agenzie federali statunitensi svolgono funzioni di *regulation*, intesa come adozione di atti a contenuto normativo equiparabili ai regolamenti amministrativi italiani e non esclusivamente di *adjudication*, ossia l'emanazione di provvedimenti amministrativi[87].

Tuttavia, se è vero che la sovranità non si esercita esclusivamente tramite i meccanismi della democrazia rappresentativa e che essa si manifesta parimenti nel dialogo con gli organi amministrativi, è vero anche che la politica intercetta un campo d'azione diverso da quello dell'amministrazione. Su questa linea direttrice si è mosso in particolare il legislatore italiano, che attraverso le riforme attuate nei primi anni Novanta, ha tentato di separare politica e amministrazione, al fine di garantire l'effettività del principio di imparzialità, sancito dall'art. 97 della Costituzione[88]. L'istanza di divaricazione tra politica e pubblica amministrazione non costituisce neppure il *core* del FOIA svedese, che – come si è detto – nasce come strumento di controllo del potere politico e riconosce ai cittadini un diritto di accesso quasi illimitato ai documenti detenuti dalle autorità pubbliche.

Eppure le legislazioni in materia di libertà di informazione rimandano sempre alla relazione tra cittadino e potere e alla modalità del suo esercizio.

Dalle esperienze prese in considerazione sono emerse delle criticità relative ai profili attuativi del diritto di accesso, che non sempre sono riconducibili a deficit nella costruzione o implementazione dell'architrave normativo[89]. Si sa: proclamare un diritto non corrisponde ad assicurarne l'osservanza, l'effettività e l'applicazione, occorrono istituzioni che incarnino una volontà politica.

Del resto, come afferma lucidamente Stefano Rodotà: «parlando di diritti bisogna sempre guardare lontano, frequentare il futuro non rimanere prigionieri del passato. E bisogna avere in essi una fede appassionata, magari ingenua, che sostenga lo sforzo continuo di una costruzione dei diritti sempre incompiuta, sempre insidiata dai nemici della libertà»[90].

anche da Testa 2019, p. 611. In relazione al segreto di Stato si veda la sentenza *U.S. v. Zubaydah et Al*. No 20-287, 2022.

87. Per un approfondimento sul tema si veda: Galetta 2016, p. 44.

88. Sul nesso tra la trasparenza, la democraticità e l'imparzialità dell'amministrazione, si rinvia a Colapietro 2014, p. 20.

89. Si rinvia in particolare ai paragrafi 5 e 7 in riferimento al modello statunitense e francese. In riferimento al modello italiano si veda Notari 2018.

90. Rodotà 2012, p. 76.

Riferimenti bibliografici

C. Alberti (2003), *La disciplina del diritto di accesso nel post Amsterdam tra consacrazione e limitazione*, in "Rivista italiana di diritto pubblico comunitario", 2003, n. 1

U. Allegretti (2009), *L'amministrazione dall'attuazione costituzionale alla democrazia partecipativa*, Giuffrè, 2009

M.R. Allegri (2014), *Democrazia, controllo pubblico e trasparenza dei costi della politica*, in "federalismi.it", 2014, n. 9

ANAC (2016), *Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013*, Delibera n. 1309 del 28 dicembre 2016

G. Arena (1979), *Diritto all'informazione e pubblica amministrazione*, Tipografia Veneziana, 1979

R. Bifulco, M. Cartabia, A. Celotto (a cura di) (2001), *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione Europea*, il Mulino, 2001

P. Calamandrei (1996), *Costituzione e leggi di Antigone*, Sansoni, 1996, p. 123 ss.

E. Carloni (2022), *Il paradigma trasparenza. Amministrazioni, informazione, democrazia*, il Mulino, 2022

E. Carloni (2009), *La "casa di vetro" e le riforme. Modelli e paradossi della trasparenza amministrativa,* in "Diritto pubblico", 2009, n. 3

E. Casetta (1977), *La partecipazione dei cittadini alla funzione amministrativa nell'attuale ordinamento dello Stato italiano*, in G.M. Rigamonti (a cura di), "La partecipazione popolare alla funzione amministrativa e l'ordinamento dei consigli circoscrizionali comunali", Atti del XXII Convegno di Studi di Scienza dell'Amministrazione di Varenna (23-25 settembre 1976), Giuffrè, 1977

A. Cauduro (2017), *Il dibattito di accesso a dati e documenti amministrativi come promozione della partecipazione: un'innovazione limitata*, in "Diritto amministrativo", 2017, n. 3

S. Cassese (2007), *La partecipazione dei privati alle decisioni pubbliche. Saggio di diritto comparato*, in "Rivista trimestrale di diritto pubblico", 2007, n. 1

M.P. Chiti (a cura di) (2013), *Diritto amministrativo europeo*, Giuffrè, 2013

M.P. Chiti (1977), *Partecipazione popolare e pubblica amministrazione*, Pacini, 1977

L. Cicatiello, E. De Simone, F. Di Mascio et al. (2022), *Exploring patterns of implementation of the Freedom of Information Act (FOIA) in local government: the case of Italy*, in "Etica pubblica", 2022, n. 2

M. Cocconi (2010), *La partecipazione all'attività amministrativa generale*, Cedam, 2010

C. Colapietro (2014), *Trasparenza e democrazia: conoscenza e/è potere*, in L. Califano, C. Colapietro (a cura di), "Le nuove frontiere della trasparenza nella dimensione costituzionale", Editoriale Scientifica, 2014

D.L. Cullier, C.N. Davis (2010), *The Art of Access: Strategies for Acquiring Public Records*, CQ Press, 2010

M. Dandelot (2018), *Évolution et enjeux du droit d'accès aux documents administratifs depuis la loi du 7 octobre 2016 pour une République numérique*, in "Revue française d'administration publique", 2018/1, n. 165

N. Durante (2018), *Pubblicità, trasparenza e FOIA: indicazioni operative*, in "italiAppalti", 2018

P. Falletta (2016), *Il* freedom of information act *italiano e i rischi della trasparenza digitale*, in "federalismi.it", 2016, n. 23

M. Filice (2019), *I limiti all'accesso civico generalizzato: tecniche e problemi applicativi*, in "Diritto amministrativo", 2019, n. 4

S. Foà (2017), *La nuova trasparenza amministrativa*, in "Diritto amministrativo", 2017, n. 1

H.N. Foerstel (1999), *Freedom of information and the right to Know*, Greenwood Press, 1999

D.-U. Galetta (2016), *Per un nuovo rapporto tra cittadino e pubblica amministrazione: un'analisi storico-evolutiva, in una prospettiva di diritto comparato ed europeo*, in "Rivista italiana di diritto pubblico comunitario", 2016, n. 5

G. Gardini (2014), *Il codice della trasparenza: un primo passo verso il diritto all'informazione amministrativa*, in "Giornale di diritto amministrativo", 2014, n. 8/9

J.M. Gimeno Feliù (2014), *El derecho de acceso a la información pública*, Civitas, 2014

W. Ginsberg (2015), *The Freedom of Information Act (FOIA): Background, Legislation and Policy Issues*, Congressional Research Service, 2015

F. Gorgerino (2022), *L'accesso come diritto fondamentale e strumento di democrazia: prospettive per la riforma della trasparenza amministrativa*, in "federalismi.it", 2022, n. 5

J.A. Guardiola (2018), *La transparencia administrativa: el acceso a la información pública*, Aranzadi, 2018

E. Guichot Reina (2014), *Transparencia, acceso a la información pública y buen gobierno*, Tecnos, 2014

M.E. Halstuk, B.F. Chamberlin (2006), *The Freedom of Information Act 1966-2006: a retrospective on the rise of Privacy protection over the public interest in knowing what the government's up to*, in "Communication Law & Policy", vol. 11, 2006, n. 4

S. La Piscopìa (2016), Italian Freedom of Information Act*: approcci interpretativi e dottrinari*, in "Rassegna della giustizia militare", 2016

F. Levi (1977), *Partecipazione e organizzazione*, in "Rivista trimestrale di diritto pubblico", 1977, n. 4

M. Lipari (2019), *Il diritto di accesso e la sua frammentazione dalle legge 241/1990 all'accesso civico: il problema delle esclusioni e delle limitazioni oggettive*, in "federalismi.it", 2019, n. 17

A. Loiodice (1969), *Contributo allo studio sulla libertà di informazione*, Jovene, 1969

O. Mir Puigpelat (2017), *El acceso a la información pública en la legislación española de transparencia: crónica de un cambio de paradigma*, in "Revista Catalana de dret públic", 2017, n. 55

M. Luciani (2001), *Il paradigma della rappresentanza di fronte alla crisi del rappresentato*, in N. Zanon, F. Biondi (a cura di), "Percorsi e vicende attuali della rappresentanza e della responsabilità politica", Giuffrè, 2001

M. Lunardelli (2023), *La trasparenza negli Stati Uniti e in Italia. Un'analisi comparata*, Editoriale Scientifica, 2023

A. Marchetti (2021), *L'esperienza virtuosa della rule of law nell'ordinamento svedese: tra storiche eredità culturali e nuovi presidi formali di legalità*, in "federalismi.it", 2021, n. 23

B.G. Mattarella, M. Savino (2018), *L'accesso dei cittadini. Esperienze di informazione amministrativa a confronto*, Editoriale Scientifica, 2018

T. Mendel (2003), *Freedom of information: A comparative legal survey*, Unesco, 2003

H. Michel (2022), *Transparency in the UE system of governance: the successes and pitfalls of a new pre-requisite for democracy*, in "Etica pubblica", 2022, n. 2

A. Moliterni (2019), *La natura dell'accesso civico generalizzato nel sistema di trasparenza nei confronti dei pubblici poteri*, in "Diritto amministrativo", 2019, n. 3

S. Nevelow Mart, T. Ginsburg (2014), *[Dis]-Informing the people's discretion: judicial deference under the national security exemption of the Freedom of Information Act*, in "Administrative Law Review", vol. 66, 2014, n. 4

F. Notari (2018), *Le criticità di un primo monitoraggio del FOIA italiano: il ruolo di Anac, Garante privacy e giudici amministrativi*, in "federalismi.it", 2018, n. 18

V.I. Österdahl (2016), *Between 250 years of free information and 20 years of EU and Internet*, in "Etikk i praksis – Nordic Journal of Applied Ethics", 2016

R. Picard (2013), *La Commission d'accès aux documents administratifs (CADA) en France*, in "Droit administratif", 2013, n. 3

J.L. Piñar Mañas (2015), *La protección de datos personales y el drecho de acceso a la información pública*, Lex Nova, 2015

A. Porporato (2017), *Il nuovo accesso civico generalizzato introdotto dal d.lgs. 25 maggio 2016, n. 97 attuativo della riforma Madia e i modelli di riferimento*, in "federalismi.it", 2017, n. 12

R. Ratish (2007), *Democracy's Backlog: The Electronic Freedom of Information Act Ten Years Later*, in "Rutgers Computer and Technology Law Journal", vol. 34, 2007, n. 1

J.J. Rivas Martínez (2019), *El derecho de acceso a la información en España: una aproximación jurisprudencial*, Aranzadi, 2019

S. Rodotà (2012), *Il diritto di avere diritti*, Laterza, 2012

L. Rossi, P. Vinagre e Silva (2017), *Public Access to Documents in the EU*, Hart Publishing, 2017

M.A. Sandulli, L. Droghini (2020), *La trasparenza amministrativa nel FOIA italiano. Il principio di conoscibilità generalizzata e la sua difficile attuazione*, in "federalismi.it", 2020, n. 20

M. Savino (2016), *Il FOIA italiano. La fine della trasparenza di Bertoldo*, in "Giornale di diritto amministrativo", 2016, n. 5

S.M. Sisto (2021), *L'importanza della trasparenza amministrativa nella prevenzione e nel contrasto alla corruzione*, Edizioni Scientifiche Italiane, 2021

L. Testa (2019), *«Ma in America questo non si può». La lotta alla public corruption negli Stati Uniti*, in "DPCE online", 2019, n. 1

C. Tommasi (2018), *Il diritto di accesso nell'ordinamento dell'Unione Europea: trasparenza o opacità amministrativa*, in Gruppo di Pisa, "Atti del seminario annuale con i dottorandi in materie gius-pubblicistiche", 2018

C. Tommasi (2018), *Le prospettive del nuovo diritto di accesso civico generalizzato*, in "federalismi.it", 2018, n. 5

R. Ursi (2016), *Le stagioni dell'efficienza. I paradigmi giuridici della buona amministrazione*, Maggioli, 2016

R. Villata (1987), *La trasparenza dell'azione amministrativa*, in "Diritto processuale amministrativo", 1987, n. 4

V. Zeno-Zencovich (2009), voce *Diritto di informazione e all'informazione*, in "Enciclopedia Italiana", XXI Secolo, 2009

J. Ziller (2019), *Accès aux documents administratifs: droit interne et droit européen*, in "Revue française de droit administratif", 2019, n. 2

J. Ziller (2005), *Commento all'art. II - 102 Cost. UE*, in L. Burgorgue-Larsen, A. Levade, F. Picod (a cura di), "Traité établissant une Constitution pour l'Europe: Tome 2, La Charte des droits fondamentaux de l'Union", Bruylant, 2005

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0139 • articolo sottoposto a peer review • pubblicato in anteprima il 22 mag. 2024

Stefano Bruno Grenci

Le applicazioni di Intelligenza artificiale a supporto dell'automazione del procedimento amministrativo

La digitalizzazione del procedimento amministrativo è da considerarsi qualcosa di ormai ineludibile che si concretizzerà pienamente, con più o meno celerità nei prossimi anni, con la naturale evoluzione delle tecnologie e delle scienze informatiche, tuttavia l'automazione completa e/o parziale di processi e procedimenti amministrativi basata sull'impiego dell'Intelligenza Artificiale (IA) non è per nulla scontata. Si consideri infatti che già solo l'adozione di algoritmi "tradizionali", ovvero non necessariamente di IA, per supportare la Pubblica Amministrazione in fasi procedimentali più o meno complesse, anche non decisorie, rappresenta ancora oggi quasi una sfida, culturale e di legittimità amministrativa e giuridica. Nel mentre, la percezione diffusa è che invece qualcosa di rivoluzionario si sia ormai messo in moto, che riguarda anche l'impiego dell'algoritmica (e dell'IA) per l'incremento della produttività e dell'efficacia dell'azione amministrativa. Una trasformazione epocale e in itinere quella della nostra PA che tuttavia, nell'avanzare, deve necessariamente coniugare la tutela dei diritti dei cittadini con i vantaggi offerti dalla tecnica, fabbisogno che questo lavoro si propone di affrontare, in termini di analisi e di approfondimenti, con una visione ibrida, possibilmente in simbiosi tra il diritto e l'informatica.

Trasformazione digitale – Procedimento amministrativo – Pubblica amministrazione – Automazione Algoritmi – Intelligenza artificiale

Artificial intelligence applications to support the automation of the administrative procedure

The digitalization of administrative procedures is to be considered as something now unavoidable that will fully materialize, with more or less speed in the coming years, with the natural evolution of technologies and computer sciences; however, the complete or partial automation of administrative processes and procedures based on the use of Artificial Intelligence (AI) is by no means a given. Infact, it should be considered that even the adoption of "traditional" algorithms, i.e., not necessarily AI-based, to support Public Administration in more or less complex procedural stages, even if not decision-making, still represents today almost a challenge, both in cultural and legitimacy perspectives. Meanwhile, the widespread perception is that something revolutionary has now been set in motion, which also concerns the use of algorithms to increase the productivity and effectiveness of administrative action. An epochal and ongoing transformation which, however, as it progresses, must necessarily combine the protection of citizens' rights with the advantages offered by technology, a need that this paper aims to address, in terms of analysis and insights, with a hybrid vision, possibly in symbiosis between law and information technology.

Digital transformation – Administrative procedure – Public Administration – Automation – Algorithm Artificial Intelligence

L'Autore è informatico, consulente tecnologico senior presso il Formez PA

1. Algoritmi, intelligenza artificiale, decisioni e diritto: un'introduzione

L'algoritmo, termine sconosciuto ai più fino ad una decina di fa, è divenuto negli ultimi tempi il protagonista assoluto di ogni argomentazione riguardante l'applicazione delle tecnologie informatiche in ogni ambito, sociale, economico e giuridico oltre che scientifico ovviamente.

La vertiginosa crescita di interesse verso gli algoritmi è stata notoriamente indotta dall'esplosione e dalla pervasività delle applicazioni degli stessi nel campo della c.d. Intelligenza Artificiale (IA), settore nel quale gli algoritmi di Machine Learning (ML) e in particolari quelli di Deep Learning (DL) si sono rivelati quasi rivoluzionari in termini di efficacia ed efficienza rispetto all'applicazione che di questi se ne poteva fare fino a pochi anni or sono.

Ancora privo di una concisa definizione normativa, l'algoritmo trova spazio solo recentemente nella giurisprudenza amministrativa (anche se ampiamente disquisito in dottrina) a seguito di alcuni importanti pronunciamenti del Consiglio di Stato, in circostanze che riguardano la sua applicazione come automa decisorio o nel caso in cui sia dirimente la sua definizione per finalità contrattuali.

La prima definizione di algoritmo appare solo nel 2019, con la sentenza n. 2270 della VI sezione del Consiglio di Stato, allorquando si deve argomentare e decidere in merito all'utilizzo che il Ministero dell'Istruzione dell'Università e della Ricerca fece di un software (nel 2015) per determinare le graduatorie dei docenti delle scuole superiori. Nella disposizione, l'algoritmo viene definito come «una sequenza ordinata di operazioni di calcolo» (definizione molto approssimativa), considerato come «in grado di valutare e graduare una moltitudine di domande» ed elemento fondamentale per la «automazione del processo decisionale». Un'ulteriore definizione che riguarda gli algoritmi è contenuta nella sentenza n. 7891/2021 del Consiglio di Stato che, esprimendosi in un contenzioso in materia di appalti pubblici, ha ritenuto necessario fare in qualche modo chiarezza su cosa si debba intendere quando ci si riferisce ad un algoritmo di Intelligenza Artificiale rispetto ai casi in cui debba considerarsi il c.d. algoritmo "tradizionale"[1].

1. La sentenza richiama il precedente pronunciamento del TAR Lombardia sez. II n. 843/2021 per il quale il termine algoritmo «richiama, semplicemente, a una sequenza finita di istruzioni, ben definite e non ambigue, così da poter essere eseguite meccanicamente e tali da produrre un determinato risultato (come risolvere un problema oppure eseguire un calcolo e, nel caso di specie, trattare un'aritmia)».

Notevole invece è stato il contributo della dottrina sulla definizione concettuale degli algoritmi nel diritto e sulla loro applicazione nei processi decisionali della pubblica amministrazione, alcuni contributi addirittura possono essere fatti risalire a oltre cinquant'anni fa, nei quali si argomentava nientemeno sulla composizione automatica di testi giuridici attraverso l'impiego di algoritmi[2]. A questo si aggiunsero inevitabilmente tanti altri contributi nei decenni successivi, soprattutto per ciò che concerne analisi e riflessioni sul ruolo e sull'applicazione dell'informatica nel diritto e sul funzionamento della pubblica amministrazione.

In questa sede, tuttavia, è l'algoritmo nella sua qualificazione informatica che interessa approfondire, soprattutto nella sua funzione principale che è quella di risolvere un "problema", con il fine di indagarne le implicazioni e le possibili conseguenze del suo impiego nel diritto. L'IA, vedremo, è un corollario dell'intera discussione. Sebbene infatti sia indubbiamente importante convergere verso una definizione giuridica dell'algoritmo sufficientemente valida e oggettiva, la portata di qualsivoglia definizione non può prescindere dalla natura scientifica propria di questo ausilio della tecnica, ormai "pietra angolare" nella rinnovazione del diritto in ambito pubblicistico e privatistico.

2. Problemi, formalizzazione e calcolabilità

Che sia considerata sufficientemente completa o meno la definizione giurisprudenziale di cui sopra, o siano più consone e appropriate le diverse altre formulazioni offerte dalla dottrina e dalla letteratura scientifica negli ultimi decenni[3], è senza dubbio fondamentale comprendere quale possa essere il perimetro di applicazione dell'algoritmica al diritto (e nel nostro caso conseguentemente all'azione amministrativa), rispetto all'aspirazione sempre più diffusa di delegare alla macchina compiti svolti dall'essere umano.

La questione, già nota sul piano strettamente informatico per ciò che riguarda la calcolabilità e la complessità degli algoritmi[4], è anche significativamente dibattuta in dottrina giuridica e interessa da vicino la formalizzazione degli algoritmi stessi e la possibilità che questi strumenti della tecnica possano sostituire l'uomo, traendo formidabile beneficio dalla sempre più crescente capacità di calcolo delle macchine.

Secondo autorevoli studiosi, l'impiego degli algoritmi è di per sé limitato nella possibilità di poterli applicare in tutti quei casi in cui è oggettivamente discrezionale l'interpretazione della norma, nei casi in cui si possano configurare più scelte tra possibili soluzioni, oppure davanti all'impossibilità di formalizzare, tradurre, codificare, il comportamento dell'algoritmo perché la norma esprime "concetti giuridici indeterminati"[5] espressi peraltro attraverso il linguaggio naturale.

Si pensi ad esempio a tutte quelle situazioni per le quali si avrebbe necessità di determinare, attraverso un automatismo algoritmico, qualità estetiche come la "bellezza", concetti astratti come "utilità pubblica", "urgenza" o "opportunità", o addirittura pensare di poter codificare in qualche modo comportamenti da parte di una macchina

2. Cfr. Gallizia-Maretti 1974.
3. Si veda Borruso 1988, p. 183 ss., dove si definisce che «l'algoritmo è una successione finita di passi (intesi come "istruzioni") ognuno dei quali definito ed eseguibile, che opera sui dati producendo risultati». Anche in Masucci 1993 l'a. definisce l'algoritmo come «un certo processo di ragionamento usato» per la risoluzione di un problema. Per la scienza informatica, è sufficientemente completa la definizione in Ferragina-Luccio 2017, p. 10 ss., dove si definisce l'algoritmo come «una sequenza finita di passi elementari che portano alla risoluzione di un problema; in aggiunta un algoritmo soddisfa le seguenti proprietà: (1) è utilizzabile su diversi input generando i corrispondenti output; (2) ogni passo ammette un'interpretazione unica ed è eseguibile in tempo finito; (3) la sua esecuzione si ferma qualunque sia l'input».
4. Su questo punto, in Ferragina–Luccio 2017, p. 9 ss., si evidenzia l'importanza di non considerare l'algoritmo come uno mezzo per risolvere qualsivoglia problema: «esistono funzioni che non ammettono algoritmi di calcolo perché tutti gli algoritmi possibili sono meno di tutte le funzioni possibili. Ovvero devono esistere funzioni non calcolabili, e devono essere l'assoluta maggioranza fra tutte le funzioni possibili».
5. Cfr. Masucci 1993: «Impossibilità di applicare mediante computer normative che contengono concetti giuridici indeterminati».

che siano oggettivamente considerati morali o etici. Per non parlare poi di tutte quelle valutazioni di merito nell'applicazione delle norme che potrebbero divenire mutevoli nel tempo o della difficoltà di codificare un algoritmo che "soppesi politicamente" la portata di alcune decisioni ovvero agisca in funzione del bilanciamento di interessi contingenti purché legittimi[6].

Insomma, emerge chiaramente che sussistono problemi di cui non vi può essere certezza di risoluzione algoritmica nel diritto, e proprio in questo senso, la *calcolabilità del diritto*, intesa come l'ambizione di poter avere la perfetta prevedibilità delle conseguenze giuridiche di atti o fatti, viene anche considerata irrealistica[7].

Ma è altrettanto vero che il mondo è denso di problemi per i quali le macchine possono aiutare (e a volte sostituire) l'uomo, soprattutto per ciò che riguarda compiti meccanici e ripetitivi ed anche per quelli complessi e articolati, purché sia univocamente chiaro l'obiettivo da raggiungere.

Su questo fronte è evidente l'incessante avanzata dell'informatizzazione della pubblica amministrazione (compresa l'amministrazione della giustizia), soprattutto per ciò che riguarda la digitalizzazione degli atti e dei processi interni, che contempla sovente l'impiego di algoritmi finalizzati all'automazione di compiti (spesso banali e ripetitivi) che sono conseguenza dell'applicazione delle norme.

Sulla base di queste doverose premesse dedicate alle possibilità di formalizzazione degli algoritmi nel diritto, cerchiamo di analizzare e condensare quali sono le principali questioni dibattute per ciò che concerne la struttura e il funzionamento degli algoritmi stessi rispetto all'opportunità di impiegarli per l'automazione di norme o delle azioni amministrative che da queste ne scaturiscono.

3. Classi di algoritmi e trasparenza giuridica

Le modalità con cui gli algoritmi organizzano i dati di input e li elaborano per ottenere un determinato risultato non sono invarianti, se valutate rispetto all'obiettivo di realizzare automazioni che riflettano un comportamento il più idoneo, comprensibile e coerente possibile con l'applicazione tradizionale di una norma da parte di un soggetto legittimamente competente.

Gli algoritmi, in base al problema da risolvere, possono essere progettati per adoperare tecniche di calcolo molto sofisticate e molto complesse da comprendere per i non addetti ai lavori, come ad esempio le tecniche che prevedono l'impiego di *reti neurali artificiali* utilizzate dagli algoritmi di deep learning nei sistemi di IA. Ancor di più, gli output prodotti dall'elaborazione effettuata dagli algoritmi di IA possono risultare inspiegabili addirittura agli stessi sviluppatori che li hanno realizzati.

Nel corso degli ultimi decenni gli studiosi del diritto si sono diffusamente interessati a come gli algoritmi computano le loro elaborazioni e, già molto tempo addietro, un'autorevole dottrina[8] postulava la necessità che queste procedure di calcolo fossero opportunamente congegnate in modo tale da evidenziare un funzionamento ricostruibile secondo lo schema "*Se* si verifica una certa situazione, *Allora* ad essa si collega un determinato effetto

6. Cfr. Civitarese Matteucci-Torchia 2016, p. 9. Per gli a. la tecnificazione deve confrontarsi con «un aspetto dell'amministrazione che è centrale a essa pur essendo forse il più sfuggente e denso di problemi, quello della sua politicità, ossia del contenuto politico delle decisioni che sono a essa richieste. Nonostante tutti i tentativi di sterilizzare o esorcizzare questo aspetto, mediante per esempio l'impiego e l'affinamento della nozione di discrezionalità amministrativa, è comunemente accettato che le autorità amministrative compiano scelte che definiscono assetti di interessi. La legittimazione di queste scelte viene normalmente ricercata o nella indiretta appartenenza delle pubbliche amministrazioni al circuito democratico e quindi riconoscendone più o meno apertamente il carattere politico (art. 95 Cost.) o nella specifica qualità tecnico-specialistica delle persone che assumono tali decisioni, enfatizzando talvolta il fatto che tale qualità è appositamente garantita mediante una formale estraneità dal circuito dell'indirizzo politico.»
7. Cfr. Zaccaria 2020.
8. Cfr. Fameli 1984, p. 145. Per l'a. la norma che esprime un contenuto prescrittivo, collega a una certa situazione tipica o ipotesi (fattispecie giuridica astratta) un determinato effetto giuridico (modificazione della realtà giuridica). In questo senso essa si configura come una regola di tipo condizionale (If...Then: se si verifica una certa situazione, allora ad essa si collega un determinato effetto giuridico).

giuridico". Uno schema che, seppur non esaustivo[9], individua un modello concettuale di costruzione degli algoritmi basato sul *nesso di causalità* che si ritiene, ancora oggi, possa agevolare, o meglio, possa essere un presupposto abilitante per l'automazione di quelle norme la cui "architettura" configura un principio di applicazione causa-effetto.

L'attenzione su questo tema però, a ben vedere, emerge non solo come una questione di forma o di struttura ma riguarda da vicino il problema più generale della conoscibilità del processo attuato dall'algoritmo, riguarda in particolare il tema della trasparenza del funzionamento dell'automa e, come diretta conseguenza, riguarda la possibilità di poter desumere dal comportamento dell'algoritmo le motivazioni che lo hanno condotto a determinare un certo risultato piuttosto che un altro.

Sostanzialmente siamo di fronte al cuore del problema che riguarda l'applicazione degli algoritmi ai processi decisionali in ambito giuridico e, in particolare, a ciò che riguarda l'automazione dei procedimenti amministrativi, rispetto al quale, i contributi giurisprudenziali introdotti con la nota sentenza del Consiglio di Stato n. 2270/2019 rappresentano un vero spartiacque. I giudici, pur incoraggiando e promuovendo il lodevole intento del Ministero sull'utilizzo di procedure informatiche (ovvero di algoritmi) per la determinazione automatica delle graduatorie dei docenti, intervengono censurando tale amministrazione sulla mancanza di trasparenza, ammonendo che «l'utilizzo di procedure "robotizzate" non può, tuttavia, essere motivo di elusione dei princìpi che conformano il nostro ordinamento e che regolano lo svolgersi dell'attività amministrativa».

E uno di questi principi è chiaramente la trasparenza, motivo per cui la sentenza sottolinea conseguentemente che la "regola algoritmica", in quanto tale, «possiede una piena valenza giuridica e amministrativa, anche se viene declinata in forma matematica, …» e, proprio in virtù di questa proprietà giuridica, questa regola debba soggiacere ai principi di «pubblicità e trasparenza (art. 1, l. 7 agosto 1990, n. 241), di ragionevolezza, di proporzionalità, ecc.».

A rafforzare ancor di più questa indiscutibile necessità di comprendere il comportamento di un automa che agirebbe per nostro conto, sempre nella sentenza viene definitivamente statuito che «l'algoritmo, ossia il software, deve essere considerato a tutti gli effetti come un "atto amministrativo informatico"», affermazione chiaramente densa di conseguenze sul piano della possibilità di approfondire senza limiti di sorta il funzionamento algoritmico.

E infatti i giudici scrivono che «la decisione robotizzata (ovvero l'algoritmo) deve essere "conoscibile", secondo una declinazione rafforzata del principio di trasparenza, che implica anche quello della piena conoscibilità di una regola espressa in un linguaggio differente da quello giuridico», ma non basta, perché in questo modo diviene chiarissimo l'intento giurisprudenziale di introdurre le basi sulla sindacabilità del risultato proposto dall'algoritmo, infatti viene palesemente enunciato che il fine è quello di «poter verificare che gli esiti del procedimento robotizzato siano conformi alle prescrizioni normative 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 imposto»[10].

La sentenza del Consiglio di Stato, definitivamente, appare come una più ampia dissertazione del principio esposto dal Considerando 71 del Regolamento (UE) 2016/679 (GDPR), per il quale, sulla questione del trattamento dei dati e sulle decisioni automatizzate, evidenzia che «…In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione

9. Cfr. Masucci 1993. L'a. sottolinea la situazione che limita l'applicazione dello schema "Se…Allora", osservando che «in alcuni casi nella norma non è riscontrabile affatto lo schema del giudizio condizionale. Ciò accade, in particolare, quando la norma non si limita a prevedere un effetto, ma direttamente lo attua».

10. La sentenza del Consiglio di Stato n. 2270/2019 va oltre perché, quasi a voler introdurre indicazioni per i funzionari delle amministrazioni preposti al controllo, indica quali devono essere gli elementi che documentano la procedura informatica: «Tale conoscibilità dell'algoritmo deve essere garantita in tutti gli aspetti: dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella loro procedura valutativa e decisionale e dei dati selezionati come rilevanti».

della decisione conseguita dopo tale valutazione e di contestare la decisione». L'art. 22 comma 1 dello stesso regolamento, ancor più espressamente, sancisce che «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».

La giurisprudenza italiana e la normativa europea dunque, inevitabilmente, convergono e la "conoscibilità" diviene così indissolubilmente legata all'algoritmo come una proprietà che quest'ultimo deve necessariamente possedere, a tal punto che, diversamente, difficilmente se ne può immaginare un utilizzo applicato all'automatismo di procedimenti amministrativi, o per automatizzare decisioni sostituendo la figura del giudice[11].

E se la conoscibilità diviene un requisito fondamentale, gli algoritmi che utilizzano per la risoluzione di problemi tecniche di calcolo difficilmente comprensibili o documentabili – come ad esempio gli *algoritmi predittivi* impiegati nei sistemi di IA – nell'ambito del diritto devono essere utilizzati con le dovute cautele: un incauto utilizzo di questi algoritmi a supporto dei processi decisionali o addirittura per la diretta elaborazione di atti/provvedimenti potrebbe comportare l'inutilizzabilità dei risultati ottenuti o dare facilmente luogo a contenziosi come già avvenuto.

Di questo parleremo meglio successivamente, e porremo in risalto i significativi rischi emergenti dall'impiego congiunto di algoritmi predittivi e Big Data, componenti principali dei moderni sistemi di IA.

4. Algoritmi predittivi, intelligenza artificiale, trasparenza e decisioni

Gli algoritmi predittivi rappresentano una particolare classe di algoritmi capaci di fornire una soluzione ad un certo problema basata sull'analisi di dati storici o comunque significativi associati al problema stesso.

Dal punto di vista computazionale, la caratteristica peculiare degli algoritmi predittivi è rappresentata dal fatto che il risultato ottenuto da questi algoritmi è determinato dall'applicazione iterativa di funzioni matematiche tipicamente molto complesse, mirate all'ottenimento di una previsione.

Questi algoritmi elaborano una sequenza di istruzioni con il fine di ottenere la migliore probabilità che un certo risultato, raggiunto a partire dai dati in input, sia la migliore risposta possibile rispetto all'esigenza di interpretare una realtà che di fatto non si conosce completamente.

I moderni algoritmi di questo genere, quelli di machine learning e deep learning, godono inoltre della capacità di poter "apprendere" – con o senza l'intervento dell'uomo – ovvero di memorizzare risultati già computati e riutilizzarli per le successive elaborazioni con l'obiettivo di migliorare la qualità del risultato finale. Per questi algoritmi, inseriti in complessi sistemi di IA, la quantità e la qualità dei dati acquisiti come input è determinante rispetto alla loro capacità di poter fornire risultati il più possibile prossimi alle aspettative di precisione degli utenti.

L'IA, che impetuosamente si sta diffondendo come accadde con l'informatizzazione dopo l'avvento di Internet, è fondata dunque su algoritmi di tipo probabilistico, capaci anche di elaborare "deduzioni" senza l'intervento umano (produrre nuovi dati di input in modo autonomo), e non agisce perché opportunamente programmata con un insieme di regole che possano essere la trasposizione di una prescrizione normativa, ma procede attraverso complesse e sofisticate (imprevedibili) tecniche matematiche al riconoscimento di risultati possibili per similitudine[12], rispetto ad una miriade di casi

11. Cfr. Pietrangelo-Nannipieri 2023. Il tema della sostituzione del giudice con un automa è fonte di inevitabile contrasto con il nostro ordinamento come sottolineato dagli aa.: «La sostituzione dell'algoritmo al giudice, e cioè la scelta di affidare all'I.A. il compito di procedere ad una sorta di ragionamento inferenziale "artificiale" e sostitutivo rispetto al ruolo del giudice, sconta una serie di vizi di fondo che sembrano costituire, almeno nell'ordinamento democratico italiano, ostacoli ben difficilmente superabili. La garanzia di revisione di ogni pronuncia non definitiva, la garanzia del contraddittorio e, in buona approssimazione, l'"umanità" del giudice sembrano costituire prerogative in insanabile contrasto con alcuni sistemi di giustizia previsionali adottati in ambito extra-UE».
12. Cfr. Masucci 2022. L'a. focalizza l'attenzione su una questione di fondo: gli algoritmi, anche quelli con autoapprendimento, non possono contemplare soluzioni che non derivino dal bagaglio di conoscenze accumulate.

"concreti" contenuti nella propria base di conoscenza e precedentemente categorizzati.

Allo stato attuale, dunque, la conoscibilità del funzionamento degli algoritmi di IA e la ricostruzione delle motivazioni che questi producono, ai sensi della sentenza del Consiglio di Stato n. 2270/2019, sono da considerarsi sostanzialmente impossibili da formalizzare. L'enfatizzazione di questa situazione è particolarmente diffusa in dottrina con la nota metafora della "black box" algoritmica, con lo scopo di riferirsi agli scenari in cui non sia possibile indagare il funzionamento di una macchina perché ne viene celato o non sia possibile determinarne il meccanismo o le regole operative che la governano.

Quanto argomentato tuttavia, come evidente, non sta costituendo un limite alla diffusione dei sistemi di IA in nessun campo, neanche in quello che riguarda l'amministrazione pubblica e le decisioni automatizzate, perché sostanzialmente il procedere della tecnica è inarrestabile.

I produttori di tecnologie, da sempre stimolati dall'intraprendere nuove sfide che in apparenza vengono considerate ardue se non impossibili, sono già al lavoro per cercare di congegnare soluzioni giuridicamente sostenibili, che pongano magari già in fase progettuale l'"etica" come fulcro intorno al quale far evolvere una IA sufficientemente responsabile rispetto ai diritti fondamentali degli individui[13]: alcune soluzioni già disponibili sul mercato, ad esempio, si pregiano di offrire tecnologie ausiliare per supportare la "comprensione" dei risultati forniti dall'IA, ma di questo parleremo meglio più avanti.

Altri rischi si ritengono ulteriormente incombenti sull'impiego dell'IA nel diritto, forse più preoccupanti se non inquietanti e riguardano l'architettura stessa di questi sistemi, fortemente basati su una base di conoscenza costituita da enormi quantità di Big Data principalmente e continuatamente rastrellati attraverso le cosiddette "Very Large Online Platforms" (VLOPs) e i "Very Large Online Search Engines" (VLOSEs)[14]. Ne parleremo diffusamente nei paragrafi successivi, analizzando le implicazioni che riguardano da vicino anche la tutela dei dati personali e il diritto d'autore.

5. Big Data e IA: realtà artificiale e inconsapevolezza della conoscenza

Una decisione corretta ma inspiegabile è probabilmente molto meno pericolosa di una decisione sbagliata anche se spiegabilissima.

Se è vero che la possibilità di conoscere il funzionamento di un algoritmo sia un aspetto fondamentale del diritto, lo è forse ancor di più avere le giuste garanzie che i risultati a cui un algoritmo può giungere non siano "viziati" da fenomeni distorsivi della realtà contemplata e "calcolata" come condizione al contorno, o che la realtà stessa non sia stata infarcita di dati e informazioni illegittimamente posseduti e quindi non utilizzabili per decidere alcunché.

Entrambi i timori rappresentano oggi temi fondamentali che inquietano finanche gli Stati, preoccupati ancor di più dopo l'avvento e l'incessante ascesa nel corso del 2023 della IA generativa ChatGPT[15] che si sta diffondendo in modo

In particolare, evidenzia che «Non deve essere sottovalutato il rischio che, difficilmente il procedere per similitudini riesca a cogliere la specificità della situazione singola. Situazioni particolari, eccezioni, sono estranee alle decisioni adottate con un algoritmo che si autoregola. In questo caso la decisione finisce sempre per essere in riferimento con altre situazioni.»

13. Cfr. Pietrangelo-Nannipieri 2023. Gli aa. rilevano l'importanza di ergere la protezione dei diritti fondamentali degli individui come una misura per l'impiego etico delle applicazioni di IA, peraltro ribaditi dalle disposizioni costituzionali degli artt. 3 ("principio di uguaglianza") e 97 ("principio di buon andamento della pubblica amministrazione").
14. Commissione europea, *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*, comunicato stampa, 25 aprile 2023.
15. ChatGPT è un'implementazione di quello che in gergo tecnico viene definito come *Large Language Model* (LLM), una particolare realizzazione di intelligenza artificiale generativa (capace cioè di generare nuovi ed "originali" contenuti) specializzata per interagire con gli esseri umani attraverso la conversazione. ChatGPT, che si presenta all'utente come una "chat bot", è stato sviluppato dalla società OpenAI™ (cospicuamente finanziata da Microsoft e dal magnate Elon Musk) che lo ha reso disponibile per il libero utilizzo sul Web a partire

pervasivo in tutti i settori della società, dell'economia e della scienza.

ChatGPT, intelligenza artificiale del tipo Generative Pre-trained Transformer (GPT)[16] ha manifestato capacità strabilianti, è in grado di comprendere e rispondere alla perfezione in linguaggio naturale e fornire risultati formidabili generati "al-volo" sulla base delle richieste fornite dall'utente.

I risultati prodotti da questa IA appaiono come se gli stessi fossero realizzati da esseri umani, anzi, da esseri umani dotati di capacità straordinarie, perché ChatGPT ha la possibilità di attingere ad una banca dati praticamente infinita situata sul Web (anche sfruttando l'immensa disponibilità di dati offerta da VLOPs e VLOSEs) e gli artefatti prodotti da questa IA e dalle sue omologhe possono essere assemblati attraverso le "abilità" di sistemi dedicati al supercalcolo che divengono sempre più potenti.

La moderna IA generativa oggi è in grado di rispondere a quesiti di ogni genere, comporre poesie, creare nuove rappresentazioni di dipinti basandosi sullo stile di Leonardo da Vinci o su quello di Monet o sullo stile di entrambi (ChatGPT + Dall-E), allo stesso modo può comporre musica, risolvere problemi matematici simbolicamente, scrivere articoli scientifici, contribuire ad individuare nuovi farmaci (come avvenuto nel 2020 con la scoperta dei laboratori del MIT dell'antibatterico ad ampio spettro "Halicina", ottenuta impiegando anche "solo" algoritmi di machine learning[17]), generare codice applicativo in qualsiasi linguaggio di programmazione e generare algoritmi per la risoluzione di specifici problemi[18], analizzare e produrre previsioni finanziarie, superare il test LSAT (il test americano di ammissione alle facoltà di Legge in USA e Canada) collocandosi tra i migliori, e tante altre cose.

Tuttavia, ChatGPT e le analoghe IA generative sono pur sempre IA che, almeno per il momento, devono il loro funzionamento alla possibilità di attingere informazioni da una base di conoscenza che concretamente non è altro che un'immensa banca dati precostituita e opportunamente strutturata (categorizzata, classificata), costantemente alimentata dall'IA stessa con meccanismi di autoapprendimento che sfruttano finanche i quesiti sottoposti dagli utenti. E gli utenti sono attratti quasi ipnoticamente da questa nuova rivoluzione tecnologica perché sistemi come ChatGPT sono capaci di trasferire la percezione che si possa interagire con l'IA come se questa sia a tutti gli effetti una macchina onnisciente[19].

L'IA generativa e tutte le IA odierne basano il loro funzionamento su una realtà costruita artificialmente, i cui contenuti sono sostanzialmente impossibili da certificare e che potrebbero di conseguenza contenere dati e informazioni personali

dal 30 novembre 2022. L'introduzione di ChatGPT e dell'IA generativa in generale sta rivoluzionando l'industria tecnologica. In Malaschini 2023, l'a. in proposito evidenzia che «Può essere interessante ricordare che, nel dicembre 2022, OpenAI ha richiesto la registrazione presso lo United States Patent and Trademark Office (USPTO) dei termini GPT e ChatGTP. La richiesta non è stata accolta in quanto i due termini non sono stati ritenuti "distintivi", ma generici e descrittivi. Sono infatti utilizzati in campo informatico con riferimento ad una particolare architettura di modello».

16. L'acronimo individua l'applicazione di un particolare modello di analisi del testo (introdotto nel 2018) che ha di fatto permesso il vero salto di qualità nella comprensione del linguaggio umano. BERT (*Bidirectional Encoder Representations from Transformers*) è un ulteriore e valido modello di analisi del testo utilizzato da altri sistemi di IA generativa che viene considerato migliore in termini di capacità di comprensione del contesto e quindi del testo in generale.
17. Trafton 2020.
18. Per fornire un esempio di queste capacità (tra i tanti sicuramente presenti in letteratura), sono stati sottoposti a ChatGPT alcuni quesiti per la generazione di algoritmi che riguardano il problema relativamente semplice delle Torri di Hanoi e quello invece decisamente più complesso del tragitto sui ponti della città di Königsberg.
19. I sistemi come ChatGPT sono opportunisticamente progettati per fornire all'utente sempre una risposta, qualunque essa sia e qualsiasi senso possa avere. Gli utenti avranno quindi sempre una risposta ad un loro quesito e la responsabilità di utilizzarne il risultato sarà a loro carico, come d'altronde ben specificato dalle informative inserite nei Terms of Use di tutti questi prodotti che gli utenti stessi devono accettare per utilizzarli.

riservati, dati e informazioni tutelati dal diritto d'autore o magari sensibili per la sicurezza degli Stati o tali che, se aggregati, possano costituire una minaccia o un pericolo di qualsiasi natura; in questa realtà (aumentata e/o alterata) non è raro inoltre imbattersi in contenuti falsi (fake news), artificiosamente creati per gli scopi più disparati. Contenuti, peraltro, che logicamente sono tenuti insieme da invisibili o meglio non conoscibili relazioni, "tessute" senza alcuna regola normativa o etica da algoritmi eccezionalmente complessi che agiscono anche in modo inspiegabile dagli stessi sviluppatori dell'IA.

L'IA odierna, definitivamente, per quanto argomentato, è del tutto inconsapevole della realtà costruita e di cui è a "conoscenza" e il rischio per gli utilizzatori è che i risultati che questa è capace di offrire, in modo formidabile e quasi potremmo dire affascinante, possano basarsi su assunti che non aderiscono alla realtà dei fatti.

Eppure, sebbene oggi tutti i sistemi di IA, anche a seguito degli interventi giurisprudenziali a tutela del trattamento dei dati personali[20], mettano in guardia gli utenti rispetto ai rischi predetti, l'utilizzo di sistemi come ChatGPT sta diventando dilagante. E la diretta conseguenza di tutto ciò è il diffondersi di situazioni molto preoccupanti in tutti gli ambiti che riguardano direttamente o indirettamente il diritto, tra i quali: la tutela del diritto d'autore ovvero della proprietà intellettuale, la riservatezza di dati sensibili soprattutto in ambito di cybersecurity, la riservatezza dei dati personali, la tutela dei soggetti più fragili nell'accesso ad Internet, le fake news[21], le *hallucinations*[22], il pregiudizio[23] (o *bias*) associato ai risultati forniti dall'IA.

20. Tra questi, il n. 112 del 30 marzo 2023 del Garante per la Protezione dei Dati Personali (GPDP) può considerarsi probabilmente il più eclatante perché determinò la sospensione delle attività dell'IA "ChatGPT" sul territorio italiano per violazione del Regolamento (UE) 2016/679 e del d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) ed ebbe il merito di sollevare la questione in seno all'Unione europea che qualche settimana dopo corse ai ripari attivando una "task force" dell'*European Data Protection Board* (EDPB) a promuovere/agevolare la cooperazione e lo scambio di informazioni sulle possibili azioni di *enforcement* portate avanti dalle varie Autorità di Controllo su ChatGPT.
21. Con questo termine ci si riferisce comunemente alla presenza e alla diffusione (in particolare sul Web) di notizie false o comunque poco o per nulla aderenti alla realtà, immesse nel circuito dell'informazione perché ritenute invece vere o perché artificiosamente costruite per una finalità specifica. Il Web è letteralmente inondato dalla presenza di fake news. I sistemi di IA, che fanno largo uso di tecniche di *web-scraping* ovvero pescano/raschiano dalla rete ogni genere di contenuto utile per accrescere la propria banca dati e addestrare meglio i propri sistemi di conoscenza, possono essere significativamente influenzati dalla presenza in rete di fake news. I sistemi di IA sono ugualmente vittime di un pericolo analogo raccogliendo informazioni su qualsiasi argomento la cui fonte non sia adeguatamente verificata. In Passaglia 2020, l'a. evidenzia già in premessa quanto importante possa rivelarsi questo fenomeno per la tenuta stessa delle democrazie: «Sebbene la disinformazione sia un fenomeno antico, con lo sviluppo delle nuove tecnologie le fake news hanno ripercussioni non trascurabili finanche sul corretto funzionamento della democrazia».
22. Le cosiddette *hallucinations* sono situazioni che si verificano quando la macchina, pur di dare una risposta, fornisce contenuti "volutamente" falsi, imprecisi o irrilevanti. In Malaschini 2023, l'a. evidenzia come «Gli esempi di hallucinations sono numerosi: ricordiamo quello di un avvocato del foro di New York, Steven Schwartz, che in una causa contro la compagnia aerea AVIANCA ha citato tra i precedenti fornitigli da ChatGPT un caso Martinez v. Delta ed uno Zickerman v. KOREAN AIR, che il giudice del Tribunale di Manhattan ha riscontrato essere assolutamente inesistenti. Ed ancora, quanto accaduto al neosindaco di una cittadina vicina a Melbourne, Brian Hood, che una ricerca effettuata sempre su ChatGPT ha collegato ad una condanna per corruzione, mai avvenuta. Il che lo ha indotto a denunciare OpenAI per il danno reputazionale provocato dalla falsa notizia. Le conseguenze possono essere rilevanti, appunto, per le società proprietarie di questi sistemi: ad esempio le azioni di Alphabet Inc. sono scese in un solo giorno di 100 miliardi, quando la sua chatbot "Bard" ha commesso un errore fattuale rispondendo ad una domanda rivoltagli in occasione della sua presentazione».
23. Si legge nel sito di OpenAI: «ChatGPT is not free from biases and stereotypes, so users and educators should carefully review its content. It is important to critically assess any content that could teach or reinforce biases

Tuttavia, cerchiamo comunque di analizzare come sia possibile coniugare le applicazioni dell'IA e in generale le decisioni algoritmiche ai procedimenti amministrativi, nell'inderogabile equilibrio da mantenere tra il bisogno di perseguire un miglioramento dei servizi della PA e le garanzie e i diritti dei soggetti direttamente e indirettamente coinvolti.

6. Algoritmi e decisioni in un procedimento amministrativo

Escludere l'intervento dell'uomo dalla decisione in un procedimento amministrativo comporta investire un automa, verosimilmente un sistema di IA, perché possa prendere in carico e in autonomia adempimenti procedurali ed elaborare provvedimenti che riguardano l'accoglimento, l'istruttoria e l'esito del procedimento stesso.

Per quanto sinora argomentato, un'attività di questo genere può realizzarsi soltanto e a condizione che siano soddisfatti precisi requisiti che riguardano la natura del problema e soprattutto a patto che siano garantiti i diritti fondamentali della persona.

I numerosi contributi della dottrina e soprattutto quanto statuito con il Regolamento (UE) 2016/679, in concorrenza con i principali interventi della giurisprudenza ovvero con le decisioni del Consiglio di Stato n. 2270/2019, n. 8472/2019, n. 7891/2021, ma anche dal d.lgs. 31 marzo 2023, n. 36[24], sembrano delineare un quadro giuridico abbastanza chiaro su questo tema, anche coerente con gli aspetti squisitamente informatici esposti in precedenza, sulla base del quale possono essere tratte alcune considerazioni di sintesi.

La prima è sicuramente quella per cui, ad oggi, è sostanzialmente impraticabile una gestione completamente automatica di un procedimento amministrativo, perché invalicabile la garanzia della presenza dell'uomo, "cristallizzata" dal principio di non esclusività della decisione algoritmica nell'intero processo decisionale (HITL – human in the

or stereotypes. Bias mitigation is an ongoing area of research for us, and we welcome feedback on how to improve. …». Un famigerato caso del genere è quello che occorse nella vicenda di Eric Loomis e della sua condanna eseguita sulla base dei risultati prodotti dal sistema COMPAS.

24. Sebbene si tratti del Nuovo Codice degli Appalti e quindi riguardi i procedimenti per la pubblica aggiudicazione di lavori e forniture, i principi e le prescrizioni introdotte sono evidentemente di carattere generale per il procedimento amministrativo automatizzato, introdotto come opportunità dall'art. 19 c. 7 («Ove possibile e in relazione al tipo di procedura di affidamento, le stazioni appaltanti e gli enti concedenti ricorrono a procedure automatizzate nella valutazione delle offerte ai sensi dell'articolo 30» e particolarmente disciplinato con l'art. 30: "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. 2. Nell'acquisto o sviluppo delle soluzioni di cui al comma 1 le stazioni appaltanti e gli enti concedenti: a) assicurano la disponibilità del codice sorgente, della relativa documentazione, nonché di ogni altro elemento utile a comprenderne le logiche di funzionamento; b) introducono negli atti di indizione delle gare clausole volte ad assicurare le prestazioni di assistenza e manutenzione necessarie alla correzione degli errori e degli effetti indesiderati derivanti dall'automazione. 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. 4. Le stazioni appaltanti e gli enti concedenti adottano ogni misura tecnica e organizzativa atta a garantire che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori, nonché a impedire effetti discriminatori nei confronti di persone fisiche sulla base della nazionalità, dell'origine etnica, delle opinioni politiche, della religione, delle convinzioni personali, dell'appartenenza sindacale, dei caratteri somatici, dello status genetico, dello stato di salute, del genere o dell'orientamento sessuale. 5. Le pubbliche amministrazioni pubblicano sul sito istituzionale, nella sezione «Amministrazione trasparente», l'elenco delle soluzioni tecnologiche di cui al comma 1 utilizzate ai fini dello svolgimento della propria attività».

loop), espresso attraverso l'art. 22 del Regolamento (UE) 2016/679 e ulteriormente ribadito dal Consiglio di Stato[25].

Men che meno ciò può essere attuato attraverso l'adozione di un'intelligenza artificiale che impieghi gli attuali algoritmi di machine learning e deep learning, visto e considerato che queste tecniche di calcolo non offrono al momento i necessari requisiti di conoscibilità algoritmica e i risultati ottenibili dal loro impiego attraverso i moderni sistemi di IA, sebbene straordinari, possono essere viziati nel merito da inesattezze significative, pregiudizi morali, utilizzo improprio di dati personali, utilizzo improprio di informazioni tutelate dal diritto d'autore.

La discussione, sull'insostituibilità dell'uomo come figura di garanzia nei processi decisionali attuati attraverso le macchine, rimarrà comunque aperta. Non solo per l'irrefrenabile avanzata scientifica e tecnologica che riguarda l'informatica e le sue applicazioni (anche nei processi che riguardano la pubblica amministrazione) ma anche per fabbisogni intrinsechi delle attività quotidiane la cui gestione è ormai sempre più intermediata dalle macchine: diverse sono infatti le situazioni in cui i processi, resi digitali, difficilmente possono dimostrare efficacia se non gestiti senza contemplare la presenza dell'uomo.

Laddove, ad esempio, la latenza dell'intervento umano potrebbe pregiudicare la possibilità di godere di particolari diritti, appare anzi ragionevole introdurre meccanismi automatici che possano superare tali ostacoli. Si pensi in tal caso a quelle situazioni in cui l'utilizzo di un particolare algoritmo (da considerarsi come una predeterminazione dell'autorità procedente, ai sensi dell'art. 12 della legge 241/90) riesca a rendere maggiormente efficiente la verifica di requisiti documentali per una moltitudine di utenti richiedenti un particolare beneficio economico.

In definitiva, si sta argomentando di circostanze nelle quali la decisione esclusiva algoritmica può risultare addirittura provvidenziale rispetto al fatto di rinunciarvi per via dell'esigenza preminente di garantire la presenza/supervisione dell'uomo in una decisione automatizzata.

A ben vedere inoltre, la presenza dell'uomo non può neanche essere considerata assoluta garanzia dell'applicazione dei diritti, ragionevolmente la si può invece annoverare come opportunità per prevenire l'eventuale assunzione di decisioni errate da parte di una macchina: l'individuo coinvolto nel "loop" decisionale potrebbe non essere sufficientemente competente rispetto alla decisione da assumere o condizionare la scelta sulla base di pregiudizi di vario genere.

La questione da dirimere rimane comunque sempre quella che riguarda la motivazione delle decisioni (ovvero i risultati di un calcolo) "assunte" da un algoritmo, che necessariamente devono essere argomentate. Un algoritmo, che utilizzi o meno tecniche di calcolo di tipo probabilistico, deve poter documentare l'evoluzione computazionale in una forma giuridicamente comprensibile. Le informazioni in ingresso in un procedimento amministrativo sono tipicamente documentali, le elaborazioni (discriminazioni) algoritmiche parziali e finali che processano informazioni su tali documenti devono contestualmente produrre *spiegazioni* nell'ambito del dominio di interesse che possano esplicare il comportamento della macchina, analogamente a quanto farebbe un funzionario incaricato dell'istruttoria: il calcolo può evolversi attraverso una successione di "stati" significativi rispetto al dominio di interesse, esplicitando i risultati delle elaborazioni mediante l'impiego di ontologie che riguardano ad esempio la legittimità delle assunzioni e il rispetto dei principi giuridici.

In definitiva, in una nuova visione, algoritmica, della pubblica amministrazione, sarebbe eticamente e giuridicamente più sostenibile l'assenza umana nell'atto decisorio (a meno dei casi di esclusione esaminati in precedenza) se la macchina a questo

25. Consiglio di Stato, Sez. VI, n. 8472/2019, «15.2 … l'altro principio del diritto europeo rilevante in materia (ma di rilievo anche globale in quanto, ad esempio, utilizzato nella nota decisione Loomis vs. Wisconsin), è definibile come il principio di non esclusività della decisione algoritmica. Nel caso in cui una decisione automatizzata "produca effetti giuridici che riguardano o che incidano significativamente su una persona", questa ha diritto a che tale decisione non sia basata unicamente su tale processo automatizzato (art. 22 Reg.). In proposito, deve comunque esistere nel processo decisionale 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».

deputata fosse capace di produrre ragionevoli spiegazioni del suo operare, magari impiegando tecniche di IA per fornire tali risposte in linguaggio naturale.

Ove attuabile e sostenibile, l'automazione dell'azione amministrativa priva della supervisione umana godrebbe dei vantaggi di trasparenza ed efficacia nell'applicazione del diritto di cui si parla spesso quando ci si riferisce alla cosiddetta neutralità algoritmica.

La seconda considerazione è che viceversa l'automazione algoritmica per il procedimento amministrativo, anche priva di output sufficienti ad esplicarne il funzionamento, può essere concepita come una grande opportunità, di cui sfruttare le enormi potenzialità purché venga mediata *ex ante*[26]: l'Amministrazione procedente è incoraggiata ad utilizzarne i vantaggi, ma non può rinunciare a svolgere il ruolo di "supervisore" dei risultati prodotti dalla macchina, accompagnandone gli esiti con eventuali interventi umani a supporto delle valutazioni algoritmiche, anche a garanzia della possibilità che si possa correttamente imputare la responsabilità delle decisioni assunte dall'organo titolare del potere[27].

Siamo davanti a presupposti che chiaramente apriranno nuovi scenari di innovazione nell'amministrazione pubblica che certamente sarà costretta ad un ripensamento delle logiche operative tradizionali sullo svolgimento del procedimento amministrativo, "scollando" gli attuali processi interni basati fondamentalmente sull'intervento umano, per "incollarli" nuovamente attraverso il supporto algoritmico, anche quello dell'IA, per potenziare ed estendere le capacità umane[28].

Si consideri a tal proposito che uno scenario particolare ma di ampia portata è quello in cui l'automazione amministrativa può essere realizzata attraverso algoritmi che, per la natura dei problemi da risolvere, facilitano molto il compito di rendere trasparente la procedura automatizzata e non comportano le incertezze tipiche degli algoritmi di IA: stiamo parlando di quegli algoritmi non predittivi ovvero deterministici (semplificando), che riguardano problemi sostanzialmente banali e/o molto ripetitivi, ma particolarmente onerosi se eseguiti dall'uomo nell'economia dei tempi di gestione di un procedimento amministrativo.

In questi casi è ragionevole affermare che se è vero che l'automazione non può essere ottenuta completamente per le ragioni esposte in precedenza, la presenza e l'intervento dell'uomo per supportare l'evoluzione procedimentale può essere ridotta e mitigata significativamente come vedremo più avanti.

Del futuro, tuttavia, come sappiamo non vi è certezza e non possiamo escludere il fatto che l'IA possa evolversi tecnicamente in modo tale da superare le palesi criticità attuali sul fronte del rispetto dei diritti dell'individuo e sull'accuratezza dei risultati forniti. Alcuni tentativi in questo senso sono stati già concretamente avviati e riguardano la realizzazione di sistemi di IA costruiti (a detta dei produttori) con un'etica cosiddetta "by design" [29] e sulla possibilità che l'IA incorpori meccanismi per spiegare il suo funzionamento, ma di questo parleremo meglio più avanti.

26. Consiglio di Stato, n. 2270/2019. Per la "regola algoritmica" si individua «la necessità che sia l'amministrazione a compiere un ruolo ex ante di mediazione e composizione di interessi, anche per mezzo di costanti test, aggiornamenti e modalità di perfezionamento dell'algoritmo (soprattutto nel caso di apprendimento progressivo e di deep learning)».
27. Consiglio di Stato, n. 8472/2019, 14.1, «…occorre sempre l'individuazione di un centro di imputazione e di responsabilità, che sia in grado di verificare la legittimità e logicità della decisione dettata dall'algoritmo».
28. Molto interessanti su questo tema sono le riflessioni in Floridi 2020. Per l'a. «Oggi, l'IA che ha successo scolla la soluzione dei problemi dalla necessità di essere intelligenti per poterli risolvere. È grazie a questo scollamento che l'IA è in grado di colonizzare spazi sempre più ampi di compiti da svolgere e problemi da risolvere, ogni volta che questi possono essere trattati con successo senza comprensione, consapevolezza, sensibilità, preoccupazioni, intuizioni, significato, esperienza, eleganza, passioni, persino saggezza e tutti quegli altri ingredienti che contribuiscono a qualificare l'intelligenza umana. In breve, è proprio quando smettiamo di cercare di riprodurre l'intelligenza umana che possiamo aver successo nella risoluzione di un numero crescente di problemi con l'IA».
29. Un esempio è l'IA generativa claude costruita intorno al concetto del "costituzionalismo" *by design*.

7. L'esecuzione del software come atto amministrativo informatico

Per la nota e più volte citata sentenza n. 2270/2019 del Consiglio di Stato «l'algoritmo ossia il software deve essere considerato a tutti gli effetti come un atto amministrativo informatico».

Per effetto di questa decisione del giudice, ha valore giuridico quindi il software che implementa una procedura "robotizzata" (l'algoritmo) concepita e progettata dall'amministrazione per predeterminare evidentemente il proprio agire.

Un'affermazione importante, estremamente significativa per il rinnovamento digitale della pubblica amministrazione, tuttavia si ritiene non bastevole per esaurire le questioni che riguardano la legalità sull'uso del software nell'intera dinamica dell'automazione del procedimento amministrativo.

A ben vedere infatti, il software rappresenta la prova, un'impronta certificata, delle intenzioni con le quali l'autorità amministrativa manifesta l'indirizzo del proprio agire (attraverso regole generali), non l'azione stessa dell'amministrazione che si concretizza invece con l'esecuzione del software, che non è dunque da solo sufficiente a garantire piena conoscenza e trasparenza delle decisioni che possono essere ottenute attraverso l'applicazione di algoritmi.

La base di conoscenza che riguarda l'applicazione algoritmica dovrebbe quindi essere ampliata per comprendere tutti quegli elementi salienti che caratterizzano l'esecuzione del software, per costituire quello che potremmo definire come uno *scenario di esecuzione* ovvero un atto amministrativo informatico maggiormente esteso rispetto alla sola presenza del software.

Uno scenario dentro il quale devono essere catturati, oltre il software appunto, quantomeno le informazioni fornite in input e che istanziano la fattispecie concreta, le informazioni prodotte durante l'iter istruttorio, i risultati/provvedimenti ottenuti dall'applicazione del software, le informazioni sul monitoraggio tecnico a tempo di esecuzione del software (log). Informazioni che peraltro, secondo le previsioni degli artt. 1, 20 e 71 del d.lgs. 7 marzo 2005, n. 82 (Codice per l'Amministrazione Digitale), possono essere resi conformi e annoverati come "documenti informatici" ovvero come «documenti elettronici che contengono la rappresentazione informatica di atti, fatti o dati giuridicamente vincolanti» e quindi opponibili in giudizio.

8. Automazione del procedimento amministrativo, algoritmi e sistemi di IA

È ampiamente percepibile che il *modus operandi* della pubblica amministrazione sta già cambiando e che, tra pochi anni, forse meno di una decade, l'architettura di erogazione dei servizi amministrativi dei vari organi dello Stato avrà un'impronta prevalentemente digitale.

Processi e procedure della macchina amministrativa pubblica sono stati investiti da interventi di ammodernamento senza precedenti, lo Stato sta rendendo disponibili asset infrastrutturali e servizi digitali strategici per tutto il paese[30] che le

30. Negli ultimi anni l'attività dell'Agenzia per l'Italia Digitale (AgID), in accordo alle sue funzioni statuite in particolare dall'art. 14 del CAD, è fortemente impegnata nella realizzazione di infrastrutture e servizi digitali e nella definizione di linee guida tecnico-operative che concretamente stanno delineando la strategia di digitalizzazione del paese. Le pubbliche amministrazioni centrali e locali, per la digitalizzazione dei propri servizi e delle procedure interne, possono contare su tecnologie e infrastrutture riconosciute e legittimate: SPID e CIE per l'autenticazione degli utenti; PagoPA per effettuare i pagamenti alla pubblica amministrazione e alle società pubbliche e private convenzionate; FEA per la certificazione di validità legale dei documenti; il Sistema di Interscambio per la gestione elettronica della fatturazione; il Polo Strategico Nazionale per l'erogazione e la gestione dei proprio servizi digitali; il sistema Web Analytics Italia per il monitoraggio e l'analisi dei propri portali. Le PA possono inoltre sviluppare i propri servizi in modo omogeneo e conforme alle direttive AgID utilizzando le numerose linee guida che riguardano in particolare: la produzione, la gestione e la conservazione dei documenti informatici, l'accessibilità e l'usabilità dei servizi, l'interazione tra le diverse banche dati della pubblica amministrazione attraverso meccanismi di interoperabilità, la produzione e l'erogazione di Open Data, il design e la configurazione per la gestione della sicurezza informatica. Rilevante è inoltre la rinnovata promozione delle procedure di riuso (Capo VI del CAD) che permette alla pubblica amministrazione, dopo una ragionevole analisi del caso d'uso, di impiegare soluzioni e sistemi già

amministrazioni centrali e locali possono utilizzare per realizzare (trasformare) e/o far evolvere i propri servizi, sia quelli interni sia quelli a beneficio degli utenti. Finalmente sembra essersi avviato quel balzo verso la c.d. Pubblica amministrazione 4.0[31] i cui presupposti erano stati già a suo tempo delineati con il programma nazionale di e-government orientato all'erogazione dei servizi pubblici online[32] del 1999, dall'art. 15 del d.lgs. 7 marzo 2005, n. 82 e dieci anni dopo dall'art. 1 della l. 124/2015[33], la cui accelerazione è evidentemente favorita e sospinta dalle risorse del PNRR ma anche dalla rapidissima trasformazione tecnologica e dal successo che ruota intorno all'IA generativa.

Nonostante ciò, questo cambiamento non sembra essere stato sufficientemente supportato dal legislatore, l'emanazione di norme negli ultimi anni è stata sostanzialmente indotta dall'incessante progresso tecnologico e dalla giurisprudenza e non si è palesata una precisa e organica riforma mirata alla rinnovazione di leggi come ad esempio la legge 7 agosto 1990, n. 241 (a tale riguardo si espresse anche il Consiglio di Stato[34] nel lontano 2005) dalla cui applicazione discende la possibilità di poter garantire il principio costituzionale di buon andamento dell'azione amministrativa (art. 97 Cost.).

Un bisogno che non è da escludersi potrà magari essere soddisfatto nel breve-medio periodo, incrementalmente, sulla scorta della forte pressione esercitata dal mercato tecnologico particolarmente rinvigorito dalle entusiasmanti opportunità offerte dall'IA. Scenario che si va configurando in accordo a quel principio che vuole che le rivoluzioni tecnologiche siano portatrici di cambiamenti delle istituzioni sociali con fisiologici e reciproci adattamenti, nel solco di un percorso forse ormai tracciato, che porterà all'eliminazione della distinzione della modalità di gestione del procedimento amministrativo, sull'assunto di considerare invariante la sostanza rispetto alla forma[35].

Si ritiene invece piuttosto prematuro immaginare una rapida progressione dell'automazione algoritmica verso la completa sostituzione

utilizzate da altre amministrazioni che si ritengono confacenti al proprio fabbisogno anche se da sottoporre ad eventuali adattamenti.

31. Espressione comune in dottrina a cui fa riferimento anche la sentenza del Consiglio di Stato n. 8472/2019 che «riferita all'amministrazione pubblica e alla sua attività, descrive la possibilità che il procedimento di formazione della decisione amministrativa sia affidato a un software, nel quale vengono immessi una serie di dati così da giungere, attraverso l'automazione della procedura, alla decisione finale».
32. Cfr. D'Elia-Pietrangelo 2005.
33. La l. 7 agosto 2015, n. 124 (detta "Madia"), all'art. 1, auspica un cambio di passo, strutturale per la definizione e la gestione di procedimenti amministrativi digitali, evidenziando come sia necessario «ridefinire e semplificare i procedimenti amministrativi, in relazione alle esigenze di celerità, certezza dei tempi e trasparenza nei confronti dei cittadini e delle imprese, mediante una disciplina basata sulla loro digitalizzazione e per la piena realizzazione del principio "innanzitutto digitale" (digital first), nonché l'organizzazione e le procedure interne a ciascuna amministrazione».
34. Più precisamente osserva il Consiglio di Stato nel suo parere n. 11995/2005, punto 6, come «una delle questioni di fondo della materia in esame» è proprio «quella dei rapporti tra procedimento amministrativo e disciplina della "digitalizzazione", che il codice risolve – alquanto sommariamente – assorbendo in sé parti della disciplina, senza modificare (o limitandosi ad abrogare) la disciplina "amministrativa" delle stesse procedure». Obiezione che permane ancora oggi valida.
35. Cfr. Civitarese Matteucci-Torchia 2016, p. 10. Per gli aa., in merito all'indagine sulla tecnificazione dell'amministrazione e quindi sull'informatizzazione, vengono considerati dirimenti alcuni temi. *In primis* viene sollevata la questione «se non siamo al punto di dover già dire che non ha senso parlare di un'amministrazione digitale come distinta da un amministrazione di altro genere», evidenziando che «non è difficile prevedere che nel giro di non molti anni (agende digitali o meno) anche le "transazioni" amministrative saranno normalmente digitali e che quindi il codice dell'amministrazione digitale sarà il codice dell'amministrazione tout court». Definitivamente si osserva, sembra retoricamente, che rispetto a questa rivoluzione già in itinere, bisogna domandarsi "In quale modo, dunque, la forma muta eventualmente la sostanza".

dell'uomo nei compiti amministrativi e decisionali, che al momento, almeno per l'attuale cultura del diritto e della tutela dei diritti fondamentali della persona, non sembra essere all'orizzonte.

Procediamo dunque ad esaminare il contesto attuale che riguarda l'informatizzazione del procedimento amministrativo, vagliando le opportunità che già oggi sono disponibili per le amministrazioni per implementarne l'automazione algoritmica e la produzione di atti e documenti.

9. Informatizzazione del procedimento amministrativo: presupposti normativi e odierni approcci realizzativi

Nei rapporti tra cittadino e amministrazione pubblica la digitalizzazione delle azioni e delle procedure interne e verso gli utenti riguarda necessariamente la questione più ampia dell'informatizzazione del procedimento amministrativo disciplinato ai sensi della legge 241/90.

Il tema, già di notevole interesse per il diritto, lo è divenuto ancora di più in questo periodo storico caratterizzato dall'imponente diffusione di interventi progettuali realizzati nell'ambito di quella che oggi viene definita la "trasformazione digitale" della pubblica amministrazione. Questi interventi interessano massicciamente l'implementazione digitale di procedure interne e di procedimenti che, specialmente nell'ultimo lustro, vengono attuati seguendo in modo preponderante i dettami del d.lgs. 82/2005 e gli strumenti programmatici e operativi ministeriali e di governo[36].

L'informatizzazione in itinere può contare su solide basi normative[37] che legittimano l'operato delle amministrazioni, ma è indubbio che sul fronte della ragionevole ambizione delle stesse di munirsi di più o meno sofisticati meccanismi di automazione del procedimento istruttorio la situazione è decisamente più complessa, principalmente per via dell'assenza di una sufficiente e organica legislazione in materia che ne permetta di regolamentare l'esecuzione con l'apporto di algoritmi.

Sebbene dunque le piattaforme informatiche che le pubbliche amministrazioni oggigiorno hanno l'opportunità di realizzare possono giovarsi di tecnologie abilitanti che permettono di supportare in modo egregio le diverse fasi di un procedimento amministrativo, le dinamiche evolutive dello stesso, il livello di automatismo nelle decisioni attraverso l'impiego di algoritmi e le modalità gestionali del corredo informativo associato al procedimento non possono che divenire caratteristiche dei sistemi stabilite autonomamente dalle singole amministrazioni titolari[38].

36. I progetti in corso sono sostanzialmente "guidati" in termini programmatici e strategici dalle "missioni" del PNRR e dagli indirizzi dei programmi operativi regionali che in questo contesto sono (ad oggi) correlati agli obiettivi delineati dal "Piano Triennale per l'Informatica nella Pubblica Amministrazione 2022-2024" e dall'"Agenda per la Semplificazione 2020-2026".
37. Ai fini del corretto inquadramento normativo degli interventi, le PA si giovano di diverse importanti prescrizioni del Codice per l'Amministrazione Digitale, tra cui: l'art. 12 ("Norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa"), comma 1, che esplicita ancora meglio le prerogative costituzionali delle amministrazioni, anche nella potestà di poter utilizzare le tecnologie dell'informazione per il buon funzionamento e le garanzie dei diritti di cittadini e imprese; l'art. 15 ("Digitalizzazione e riorganizzazione"), comma 2, che individua chiaramente che gli interventi di informatizzazione di cui all'Art. 12 debbano riferirsi alla gestione del procedimento («… le pubbliche amministrazioni provvedono in particolare a razionalizzare e semplificare i procedimenti amministrativi…»); l'art. 41 ("Procedimento e fascicolo informatico"), comma 1, è invece lapidario: «Le pubbliche amministrazioni gestiscono i procedimenti amministrativi utilizzando le tecnologie dell'informazione e della comunicazione. Per ciascun procedimento amministrativo di loro competenza, esse forniscono gli opportuni servizi di interoperabilità o integrazione, ai sensi di quanto previsto dagli articoli 12 e 64-bis». Per la l. 241/90, è invece evidente l'apertura al nuovo corso dell'art. 3-*bis* ("Uso della telematica"), co. 1, introdotto dall'art. 12, co. 1, lett. b della l. 11 settembre 2020, n. 120, che rappresenta di fatto la "connessione" su questo tema con il CAD: «Per conseguire maggiore efficienza nella loro attività, le amministrazioni pubbliche agiscono mediante strumenti informatici e telematici, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati».
38. In una fase di grande fervore come quella attuale, le amministrazioni sembrano attuare un approccio molto cautelativo (considerati anche i noti provvedimenti della giustizia amministrativa sull'automatismo decisionale

Amministrazioni che quindi vedono riproporsi con maggiore forza, vista la dirompente diffusione dell'IA, un tema dibattuto da tanti anni dalla dottrina e dalla giurisprudenza e che riguarda le implicazioni (nel diritto) della mediazione delle tecnologie nel rapporto tra cittadini e pubblica amministrazione, specie nel caso in cui tutto ciò comprenda anche le dinamiche di formazione della volontà.

Oggi, tuttavia, le amministrazioni possono beneficiare di infrastrutture e tecnologie informatiche largamente sufficienti ai loro scopi, impiegare importanti servizi tecnologici gratuiti concessi dallo Stato e sfruttare non solo le incredibili potenzialità offerte dalle applicazioni algoritmiche nella formazione della decisione da parte di una macchina, ma anche le aperture legislative e giurisprudenziali in tal senso.

Seguiremo quindi ad analizzare in che modo e con quali opportunità le amministrazioni possono procedere alla costruzione degli automatismi per l'iter istruttorio, e le possibilità di addivenire alla formazione o all'elaborazione elettronica di atti e provvedimenti parziali e finali del procedimento.

10. Istruttoria algoritmica

L'istruttoria di un procedimento amministrativo, nella sua natura di problema per la cui risoluzione debbano essere espressi pareri da parte di uno o più soggetti coinvolti nel procedimento, non può contemplare un'automazione algoritmica che escluda, nel suo complesso, la presenza dell'uomo. È una risultanza di quanto si è già argomentato in precedenza sulla questione dell'applicazione degli algoritmi al procedimento amministrativo: nella fattispecie, infatti, già solo i pareri demandati agli uffici titolari degli endoprocedimenti nonché il parere conclusivo del responsabile del procedimento costituiscono decisioni, dipendenti dal contenuto delle norme, eventualmente frutto di interpretazioni e/o di discrezionalità, quindi in via generale non automatizzabili.

Nel merito inoltre dell'intera attività istruttoria, è significativo in questa direzione il parere del TAR del Lazio n. 10963/2019, che a sua volta riprende concetti espressi in precedenti decisioni, quando afferma 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 e che pertanto, 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»[39].

commentati in precedenza), riservandosi l'opportunità di sostenere con maggior favore l'informatizzazione dei procedimenti senza introdurre algoritmi di supporto alle decisioni o che addirittura producano le decisioni stesse. Sono molte diffuse infatti soluzioni nelle quali l'informatizzazione delle fasi istruttorie non comprende particolari automatismi se non la concatenazione di processi informatici finalizzati, nella migliore delle situazioni, alla simulazione del procedimento "analogico", all'acquisizione telematica dei documenti digitali associati ai pareri prodotti dai vari uffici competenti e alla generazione di documenti di supporto all'istruttoria. In questi casi i processi con i quali si evolve il procedimento sono governati passo-passo dai funzionari incaricati, che non di rado sperimentano complessità gestionali di tipo tecnico anche elevate legate ad un'informatizzazione del procedimento non proprio ottimale. Ulteriormente, il deficit cronico di competenze della PA nel settore ICT sta spingendo le stesse amministrazioni a delegare ai fornitori tecnologici molti aspetti della progettazione dei sistemi che, seppur realizzati coerentemente ai contratti in essere e in accordo alle normative vigenti, riflettono molte volte una marcata tendenza alla tecnicizzazione di azioni e processi amministrativi trasposti in versione digitale. Una delega che evidentemente rappresenta un rischio delle amministrazioni sulle possibilità che interessi diversi da quelli pubblici possano avere il sopravvento.

39. Cfr. Marongiu 2022, p. 1520. L'a. evidenzia che questa pronuncia giurisprudenziale sia importante anche per il fatto che il giudice considera che il presupposto di perfezione dell'algoritmo non debba mai costituire motivo per la sostituzione dell'intervento umano: «È opportuno osservare che questa posizione del giudice non si

Tutto ciò, tuttavia, non può e non deve allontanare la possibilità di costruire un'automazione algoritmica del procedimento e in particolare dell'istruttoria, perché la stessa, al contempo, si compone di un insieme di azioni amministrative che ne riguardano l'orchestrazione e il supporto all'evoluzione, che poco hanno a che fare con il tema della decisione affidata unicamente alle macchine e molto invece riguardano l'opportunità di contribuire all'efficientamento del funzionamento dell'amministrazione pubblica, come anche auspicato dal Consiglio di Stato e dal legislatore con l'art. 19 e l'art. 30 del d.lgs. 36/2023 (in un ottica di generalizzazione dei principi a beneficio di tutti i tipi di procedimenti, non solo di quelli che riguardano gli appalti pubblici).

In una visione, dunque, che consideri indifferente le modalità di esecuzione delle attività, l'istruttoria può essere nel suo complesso governata da un algoritmo che ne implementi un modello generale di esecuzione che, sempre sotto la supervisione del responsabile del procedimento, supporti ad esempio la sequenza delle fasi, il rispetto delle condizionalità, l'eventuale sincronizzazione di eventi, l'applicazione della tempistica, la generazione automatica di comunicazioni ai soggetti interessati dal procedimento e l'emanazione del provvedimento finale.

Una serie di azioni che, se codificate correttamente ed eseguite attraverso un algoritmo (non predittivo ovviamente), è evidente possano contribuire, strutturalmente, a rendere più effettive le finalità del procedimento amministrativo statuite dall'art. 1 co. 1 della l. 241/1990.

Nell'iter istruttorio così realizzato, l'eventuale applicazione dell'IA potrebbe addirittura rafforzare le garanzie di celerità e di qualità delle valutazioni, nei casi in cui sia possibile ovviamente automatizzare una o più fasi che, rispetto alla specificità del procedimento, contemplino ad esempio l'elaborazione di una grande quantità di dati per determinare la stima di un certo fenomeno (sociale, economico, tecnico), stima che si ritiene ovviamente necessaria per supportare l'esito finale dell'istruttoria[40].

Per l'automazione di fasi che richiedono invece la semplice esecuzione di compiti banali e/o ripetitivi su grandi quantità di dati, sono bastevoli algoritmi non predittivi ovvero che non facciano uso di tecniche di machine learning e deep learning, che

riferisce solo alla possibilità che l'algoritmo presenti disfunzioni e dunque produca elementi di illegittimità; bensì ricomprende anche l'ipotesi in cui le istruzioni del programma informatico siano perfette, ovvero "finanche ove pervengano al loro maggior grado di precisione"».

40. A tal proposito è fondamentale che l'applicazione di algoritmi sia preceduta da un'analisi che tenga in considerazione i diversi aspetti che possano inficiare i diritti dei cittadini coinvolti nel procedimento. Se da una parte il Consiglio di Stato a più riprese ha benevolmente considerato l'applicazione di algoritmi (in generale) come un'importante opportunità per la PA (sentenza n. 2270/2019, 8.1, «… l'utilizzo di una procedura informatica che conduca direttamente alla decisione finale non deve essere stigmatizzata, ma anzi, in linea di massima, incoraggiata: essa comporta infatti numerosi vantaggi quali, ad esempio, la notevole riduzione della tempistica procedimentale per operazioni meramente ripetitive e prive di discrezionalità, l'esclusione di interferenze dovute a negligenza (o peggio dolo) del funzionario (essere umano) e la conseguente maggior garanzia di imparzialità della decisione automatizzata.…» – sentenza n. 8472/2019, 8.1, «… Sempre in linea generale va richiamato quanto già evidenziato dalla sezione in ordine all'elemento positivo derivante dal nuovo contesto di digitalizzazione; in proposito, non può essere messo in discussione che un più elevato livello di digitalizzazione dell'amministrazione pubblica sia fondamentale per migliorare la qualità dei servizi resi ai cittadini e agli utenti. In tale ottica lo stesso Codice dell'amministrazione digitale rappresenta un approdo decisivo in tale direzione. I diversi interventi di riforma dell'amministrazione susseguitisi nel corso degli ultimi decenni, fino alla legge n. 124 del 2015, sono indirizzati a tal fine; nella medesima direzione sono diretti gli impulsi che provengono dall'ordinamento comunitario.») ha ugualmente messo in guardia la PA sui rischi connessi all'utilizzo di questa tecnicizzazione dei procedimenti per ciò che riguarda tutti gli aspetti particolarmente descritti nel primo capitolo di questa analisi. Nel caso di utilizzo poi di algoritmi di ML e DL è fondamentale sottolineare ancora una volta l'importanza dell'affidabilità delle banche dati che, se inficiate di inesattezze, dati contraffatti o poco esaurienti rispetti allo specifico problema, possono inevitabilmente comportare risultati errati pregiudicando i legittimi diritti degli interessati.

non destano dunque particolari preoccupazioni sul fronte dei diritti dei cittadini coinvolti nel procedimento amministrativo.

Stabilita dunque la possibilità di automatizzare l'istruttoria del procedimento nei termini appena discussi, non resta che vagliare due importanti questioni che interessano il diritto: la governance digitale di dati e informazioni associate al procedimento e i meccanismi per la generazione automatica dei provvedimenti emessi dall'autorità procedente al termine degli esiti istruttori.

Si tratta di due temi di estrema rilevanza, bisognosi di approfondimento in questa analisi, che semplificando, rappresentano rispettivamente l'input e l'output dell'iter istruttorio: una gestione non idonea di questi flussi renderebbe illegittima qualsiasi istruttoria.

11. La governance dei dati

L'informatizzazione e l'automazione di un procedimento amministrativo non possono essere legittimamente concepiti senza una corretta definizione delle modalità di memorizzazione, di trattamento, di conservazione e di gestione di dati e documenti coinvolti nel procedimento[41] sulla base di quanto previsto dal Regolamento (UE) 2016/679 (GDPR) e dal d.lgs. 10 marzo 2023, n. 24 (Codice Privacy).

A tale scopo, l'amministrazione pubblica deve adempiere alle prescrizioni che riguardano la protezione dei dati personali compresi nel fascicolo del procedimento ai sensi del GDPR, può considerarsi esentata dalla motivazione del trattamento perché lecito ai sensi dell'art. 6, co. 1, lett. e (GDPR) e dell'art. 2-*ter*, co. 1-*bis* (Privacy) e non obbligata all'indicazione delle finalità (art. 5, co. 1, lett. b, GDPR) perché palesemente di interesse pubblico, ma deve tuttavia prevedere un'organizzazione e una strutturazione dei sistemi adeguati a ottemperare al fatto che la raccolta dei dati sia adeguata, pertinente e limitata nel tempo ai sensi dell'art. 5, co. 1, lett. c del GDPR.

La pubblica amministrazione, in sintesi, deve garantire che farà un uso legittimo dei dati, li utilizzerà fino alla conclusione del procedimento, consentirà il diritto all'accesso e provvederà alla loro conservazione secondo le opportunità offerte dalla tecnica.

Garanzie che l'amministrazione pubblica, ad oggi, è in grado di poter sostenere soltanto nel caso in cui le banche dati dei propri sistemi siano ospitate all'interno di infrastrutture tecnologiche fisicamente dislocate all'interno del perimetro della comunità europea.

A tal proposito è opportuna un'ultima riflessione che riguarda i possibili impieghi dell'intelligenza artificiale nei sistemi della pubblica amministrazione: se tali sistemi sono utilizzati a supporto dell'istruttoria allora bisogna fare attenzione che gli stessi non siano coinvolti nel trattamento di dati personali perché in tal caso si dovrebbe essere certi che le loro banche dati di riferimento risiedano fisicamente in Ue.

12. Provvedimenti automatizzati

L'automazione di un procedimento amministrativo, nelle migliori delle ipotesi, può contemplare la presenza di meccanismi idonei all'elaborazione elettronica di documenti, ottenuta attraverso l'applicazione di specifici algoritmi progettati a supportare la fase istruttoria. Documenti che nella fattispecie possono essere utilizzati per comunicazioni di varia natura nell'iter istruttorio e in particolare per l'emanazione del provvedimento finale e quindi dell'output conclusivo del procedimento.

Si tratta di un'automazione che, seppur mediata dalla presenza dell'uomo come supervisore del complesso delle attività procedimentali, richiede una particolare attenzione perché il provvedimento (o qualsiasi altra determinazione intermedia con analoghe proprietà), generato di fatto da una macchina, deve essere fatto proprio dall'organo decidente e conseguentemente sottoscritto.

41. Ci si sta riferendo alla fase di acquisizione delle informazioni (dei "fatti") nell'ambito del procedimento amministrativo, prescritta in particolare dall'art. 6, co. 1, lett. a) e b) della l. 241/1990. Nel processo di costruzione dei fatti che riguardano il procedimento, l'amministrazione acquisisce dati e informazioni fornite dall'interessato che integra, a supporto dell'istruttoria, con eventuali ulteriori contributi reperibili attraverso banche dati pubbliche o riservate o direttamente sul Web. In una gestione informatica del procedimento tutto ciò richiede la realizzazione di una banca dati dai contenuti eterogenei (informazioni testuali, documenti, immagini, suoni, filmati) strutturata per supportare nel migliore dei modi le esigenze dell'amministrazione.

Per meglio chiarire questa situazione si pensi ad esempio ad un provvedimento automatizzato che un algoritmo costruisce progressivamente nel tempo e nel corso dello svolgimento dell'attività istruttoria, con l'eventuale acquisizione di pareri espressi dai diversi uffici coinvolti e con eventuali contributi prodotti da elaborazioni intermedie (magari effettuate da sistemi di IA).

Una certa dottrina[42] rappresenta una soluzione a questo problema che va nella direzione di adottare meccanismi che possono essere assimilati al concetto del "timbro e firma", applicato dagli uffici sui documenti cartacei nella catena di approvazione dell'iter istruttorio, che prevede l'impiego della tecnologia del *sigillo elettronico*[43]. Uno strumento di firma elettronica qualificata (nella versione del sigillo elettronico qualificato), conforme al Regolamento eIDAS, destinato alla sottoscrizione di documenti informatici da parte di un soggetto giuridico, che in questo caso possono essere i diversi uffici coinvolti dell'amministrazione titolare del procedimento.

Questa tecnologia ha l'indubbio vantaggio di poter essere utilizzata con un automatismo algoritmico, *suggellando* la catena di responsabilità coinvolta nell'approvazione del provvedimento, proponendolo come un atto amministrativo prodotto direttamente dall'amministrazione competente.

L'alternativa a questa soluzione permane essere quella della firma digitale conclusiva sul provvedimento finale, apposta dal funzionario, che fa propria la decisione generata tutta o in parte dalla macchina.

13. L'IA e il futuro algoritmico della pubblica amministrazione

Il percorso di analisi e di ricerca sin qui descritto si conclude con alcune riflessioni di sintesi sui possibili futuri scenari di applicazione dell'IA alla pubblica amministrazione, nonostante il campo di indagine sia ancora molto indefinito: gli stakeholder commerciali sono molto agguerriti nella difesa dei propri interessi, alcuni prodotti sembrano affermarsi più velocemente di altri, le Istituzioni governative europee stanno ancora elaborando una definitiva strategia comune. Nel mentre, gli utenti dei servizi ovvero i cittadini cercano di sfruttare quanto gli viene concesso per soddisfare le proprie necessità.

In tale scenario appare dunque interessante analizzare in chiave prospettica alcuni fattori che probabilmente potranno incidere sulle modalità di adozione dell'IA e che riguardano: l'esercizio del potere decisionale da parte delle amministrazioni pubbliche, l'evoluzione algoritmica legata all'IA, la governance dei servizi di IA da parte dei principali fornitori tecnologici mondiali.

14. Potere decisionale e algoritmi

L'esercizio del potere decisionale è una prerogativa assoluta dell'essere umano?

In un ipotetico perimetro molto più ampio del diritto, all'interno del quale la decisione algoritmica trovasse agevole applicazione (senza le insormontabili limitazioni attuali), saremmo disposti a consentire ad una macchina (ovvero ad un algoritmo) di decidere sul nostro futuro anche se questa fosse capace di spiegarci il motivo per il quale è giunta ad una determinata conclusione?

Interrogativi e riflessioni manifestati in tempi recenti anche da un'autorevole dottrina[44] che evidentemente sono mirati a fare emergere la questione di fondo, che dal futuribile è ormai divenuta di ordinaria attenzione: la sostituzione dell'essere umano con un algoritmo nelle attività giurisdizionali.

Oltre le previsioni precedentemente argomentate, sulla *calcolabilità del diritto*, sulle differenze sostanziali tra risultati certi e stime ovvero sulla predittività e sul determinismo, sul problema della motivazione correlata al concetto della black-box algoritmica, sull'imputazione delle decisioni algoritmiche, sul trattamento delle informazioni (riservatezza e tutela), il futuro delle decisioni esclusive o sempre più supportate (indotte?) dalle macchine sembra ridursi sempre più ad una questione intenzionale delle società e delle Istituzioni.

Argini all'avanzata tumultuosa della tecnica verso il dominio delle ultime prerogative dell'essere umano (e il decidere delle proprie sorti appare essere questione centrale dell'intera analisi) possono essere solidamente sollevati solo e nella misura

42. Cfr. Marongiu 2022, pp. 1521-1523.

43. Il Regolamento (UE) n. 910/2014 (eIDAS) ne disciplina l'utilizzo.

44. Cfr. Zaccaria 2020.

in cui l'etica e i principi fondamentali dei diritti degli individui potranno essere preservati da ciò che solo in apparenza si rivela in modo assoluto come conveniente e neutrale, come l'IA viene erroneamente percepita.

La pubblica amministrazione, come già detto, può significativamente giovarsi della rivoluzione algoritmica in corso, in alcuni casi anche sfruttando le incredibili capacità delle tecnologie legate all'IA, ma l'alba di questa trasformazione deve essere sapientemente guidata ovvero, deve essere sufficientemente supportata da personale competente[45] capace di incidere con adeguata autonomia sulla base di principi normativi e di regolamenti attuativi in armonia con un disegno complessivo, nazionale ed europeo, della materia.

15. Futuri algoritmici

È difficile immaginare un futuro algoritmo per la pubblica amministrazione o meglio, prospettare la possibilità di applicare automatismi ai processi amministrativi se, come abbiamo già approfondito, risulta "oscuro" (non conoscibile) il funzionamento del sistema informatico coinvolto nella decisione.

L'interessato al trattamento automatizzato (anche nei rapporti tra cittadino e amministrazione) sappiamo deve poter ottenere una spiegazione della decisione che un algoritmo ha conseguito se ciò determina effetti giuridici, e tale opportunità è realizzabile se l'intero processo di elaborazione risulta adeguatamente documentabile e comprensibile anche per i non esperti, in breve, il processo decisionale deve essere trasparente.

Ancor di più, è molto discutibile e strategicamente debole pensare di poter imporre una decisione elaborata da una macchina ai possibili beneficiari in assenza di una ragionevole motivazione che possa infonderne l'indispensabile fiducia.

Come, dunque, conciliare le grandi opportunità prospettate dal progresso di questa nuova tecnologia con le evidenti criticità in termini di trasparenza, palesemente connaturate con il funzionamento stesso degli algoritmi di machine learning e deep learning?

Per rispondere a questo fabbisogno, la ricerca scientifica[46] e l'industria tecnologica[47] nel corso degli ultimi anni hanno profuso significative energie nella definizione formale e nello sviluppo di quella che viene comunemente definita come *eXplainable Artificial Intelligence* (XAI).

L'XAI si configura concettualmente e tecnologicamente come un'introspezione nei meccanismi attuali di funzionamento dell'IA, con l'obiettivo di far emergere sufficienti informazioni utili a rendere il più possibile trasparente il processo di formazione della decisione e consentire così di poter costruire valide spiegazioni sul risultato finale prodotto dagli algoritmi di machine learning e deep learning.

Un'evoluzione dell'XAI, che vada addirittura nella direzione di imporsi come direttrice

45. Cfr. Pietrangelo-Nannipieri 2023. Sebbene l'interesse sia principalmente rivolto alla formazione legislativa, l'a. evidenzia l'importanza che la P.A. si doti stabilmente di figure professionali esperte in ambito informatico con un forte orientamento alle questioni che attengono al diritto.

46. Si evidenzia in particolare il Progetto ERC XAI - *Science and technology for the explanation of AI decision making*, che vede coinvolti la Scuola Normale Superiore di Pisa (coordinatore), l'Università di Pisa e il Consiglio Nazionale delle Ricerche. «La ricerca si concentra su come progettare la trasparenza nei modelli ML, come produrre spiegazioni controllate delle scatole nere, come rivelare i dati e gli algoritmi usati, l'iniquità e le relazioni causali nei processi. Il progetto formulerà anche standard etici e legali per l'IA». La ricerca si concentra su come progettare la trasparenza nei modelli ML, come produrre spiegazioni controllate delle scatole nere, come rivelare i dati e gli algoritmi usati, l'iniquità e le relazioni causali nei processi. Il progetto formulerà anche standard etici e legali per l'IA.

47. Alcune tra le principali industrie tecnologiche mondiali (IBM, Google, Microsoft per esempio), cogliendo la rilevanza strategica dell'impiego dell'XAI, rendono già oggi disponibili soluzioni complete e avanzate per supportare gli utenti nelle diverse fasi di impiego dell'IA. La finalità di questi prodotti è garantire un funzionamento dell'IA governabile attraverso strumenti che consentano di tenere traccia del processo decisionale, verificare l'efficacia e l'accuratezza dei risultati, comprendere la dinamica di formazione della decisione, supportando le organizzazioni nelle attività di elaborazione della motivazione delle decisioni assunte attraverso l'applicazione dell'IA.

principale di sviluppo per il potenziamento e per la nuova realizzazione di sistemi di IA, aprirebbe innegabilmente la porta al riconoscimento di queste tecnologie per un vasto impiego dell'IA anche in questioni particolarmente delicate che attengono alla tutela dei diritti fondamentali degli individui.

È un percorso quello intrapreso con l'XAI che è evidentemente virtuoso, che pone al centro l'uomo con i suoi diritti e con i suoi fabbisogni, coerente con i valori europei. Speriamo di poterne cogliere i frutti nell'immediato futuro.

16. Governance e regolamentazione dell'IA

Il paradigma di funzionamento dei moderni sistemi di IA che ci viene proposto disegna uno scenario economico e di governance ICT che reitera quello attuale: pochissime società (statunitensi) al comando per la fornitura di tecnologie da cui dipendono la vita di miliardi di persone in tutto il mondo.

L'efficacia e la potenza offerta dai migliori sistemi di IA in commercio per finalità generali (l'IA generativa dei *foundation models*, come GPT-3.5 e GPT-4.0) viene garantita da un impiego di servizi erogati in modalità SaaS[48], PaaS[49] e IaaS[50], con livelli di prestazioni che ad oggi possono essere resi disponibili solamente dalle maggiori società tecnologiche del pianeta (Google, Amazon, Microsoft, Apple, Meta (altrimenti noti come GAMAM, in aggiunta IBM storicamente impegnata nella ricerca e nella commercializzazione di sistemi di intelligenza artificiale) che ulteriormente investono monumentali risorse finanziarie per le fasi di addestramento iniziale dell'IA, per il suo sviluppo e per la gestione tecnica e organizzativa su scala mondiale. Un modello di governance che, rivelatosi già particolarmente problematico per ciò che riguarda la libera concorrenza[51] e la libertà di informazione ed espressione[52], rischia di diventare molto pericoloso se applicato all'utilizzo dell'IA: non appare un'esagerazione osservare che in poco

48. Il *Software as a Service (SaaS)* definisce un paradigma di utilizzo del software completamente diverso da quello tradizionale che prevede che il software sia memorizzato ed eseguito sul proprio computer. Un software erogato in modalità SaaS viene utilizzato da un utente con il proprio computer che lo esegue – normalmente mediante un web browser - solo ed esclusivamente attraverso la rete Internet poiché sia il codice applicativo che i dati da esso manipolati sono fisicamente memorizzati su Datacenter dislocati potenzialmente in uno o più luoghi della rete. La gestione della posta elettronica via web rappresenta una delle applicazioni SaaS più diffuse. Il paradigma SaaS rende ancora più esplicito il modello di funzionamento della computazione basato sulla rete Internet ovvero del modello definito come Cloud Computing. ChatGPT è un servizio erogato in modalità SaaS.
49. Il *Platform as a Service (PaaS)* è un paradigma basato sul modello del Cloud Computing che consente di utilizzare in locazione sistemi informatici remoti già configurati (eventualmente personalizzabili) rispetto alle proprie necessità, su cui eseguire le proprie applicazioni. Le aziende che sviluppano software, soprattutto quelle che realizzano applicazioni basate sull'IA (o personalizzazioni/addestramenti su specifici domini), acquistano servizi PaaS tipicamente da una società del club GAMAM.
50. L'*Infrastructure as a Service (IaaS)* è un paradigma basato sul modello del Cloud Computing che consente di utilizzare in locazione risorse (informatiche) remote come hardware (fisici o virtuali), spazi di memorizzazione, apparati di interconnessione e di servizi connettività, che le aziende possono utilizzare per creare veri e propri Datacenter dedicati alle proprie necessità di elaborazione. Le aziende che hanno l'ambizione di poter sviluppare ad esempio propri sistemi di IA comparabili a quelli più evoluti in commercio procedono tipicamente all'acquisto di servizi IaaS. Alcune delle società stesse del club GAMAM acquista servizi IaaS dai propri concorrenti. La Società OpenAI™ che ha realizzato come noto ChatGPT, utilizza l'infrastruttura Azure di Microsoft come anche "dichiarato" dalla stessa chatbot.
51. Per regolamentare la commercializzazione dei servizi digitali nel mercato unico europeo l'UE ha varato il Regolamento (UE) 2022/1925 – Regolamento sui mercati digitali (o *Digital Markets Act*, DMA) attraverso il quale si prefigge di garantire una reale concorrenza ad oggi minacciata dalla presenza sovrastante di pochissimi operatori economici d'oltreoceano.
52. Al fine di regolamentare la corretta circolazione delle informazioni, garantire la più ampia libertà di espressione e contrastare il dilagante fenomeno della diffusione incontrollata di informazioni false o artefatte per

tempo potremmo trovarci di fronte ad un oligopolio che deterrà il controllo del supporto alle decisioni algoritmiche e quindi delle decisioni delle società pubbliche e private di tutto il mondo, con tutto ciò che ne consegue per gli ordinamenti democratici degli Stati.

Nel disquisire quindi sulle opportunità e sul futuro dell'IA applicata alla pubblica amministrazione non si può prescindere dal tener conto dell'importanza strategica degli aspetti "architetturali" di questi sistemi, che non a caso sono diventati uno dei temi più dibattuti nelle agende dei governi degli ultimi mesi: il recentissimo e molto sofferto accordo sul regolamento per l'utilizzo dell'intelligenza artificiale in Ue (*AI Act*) testimonia non solo che gli interessi economici e geopolitici su questo terreno sono molto sentiti dai governi ma che il panorama complessivo dal punto di vista tecnico sia ancora aperto.

La regolamentazione europea sull'IA arriva in un momento cruciale e «mira ad assicurare che i sistemi di IA immessi sul mercato europeo e utilizzati nell'Ue siano sicuri e rispettino i diritti fondamentali e i valori dell'Ue»[53], tuttavia la strada da percorrere per assicurare tali obiettivi appare già particolarmente ripida. L'IA di oggi è sostanzialmente figlia di decenni di investimenti sull'attuale infrastruttura di reti, servizi, applicazioni e sistemi ad elevate prestazioni, che si sono evidentemente evoluti nella direzione di rendere abilitante su scala planetaria l'utilizzo di intelligenze artificiali delle potenzialità di ChatGPT, che si sta infatti diffondendo dappertutto con una rapidità impressionante.

I governi europei attraverso l'*AI Act* intendono perseguire il principio regolatorio secondo il quale l'adozione dell'IA debba essere sempre accompagnata da una preliminare valutazione del rischio, dalla quale devono poi determinarsi regole di impiego dell'intelligenza artificiale più o meno severe in relazione alle possibili ripercussioni sulla sicurezza degli Stati e sui diritti fondamentali dell'uomo: alcune applicazioni dell'IA sono state ritenute invece proprio "inaccettabili", come la manipolazione comportamentale cognitiva, lo *scraping* di immagini facciali non mirato, il "riconoscimento delle emozioni", il "punteggio sociale", la "categorizzazione biometrica", la "polizia predittiva".

Concludendo, sembra ormai giunto quel momento in cui alcune decisioni come quelle di porre limiti etici all'impiego delle tecnologie dell'informazione e in particolare dell'IA non possano essere più rimandate. Le società moderne diventano sempre più complesse e dipendenti dalle macchine, capaci già oggi di apprendere ed autoprogrammarsi rispetto ai propri fabbisogni operativi e degli utenti, abilità che fino a pochi anni fa erano percepite soltanto come futuribili se non fantascientifiche.

Lo scenario sembra addirittura ancora più complesso e preoccupante rispetto alle previsioni degli studiosi di qualche decennio addietro perché l'IA è stata "sapientemente" costruita dai portatori di interessi come un servizio remoto (via Internet) reso disponibile alle macchine, dominato dall'esterno e potenzialmente mutevole nel tempo, tecnicamente ingovernabile per eventuali autorità governative preposte a controlli di correttezza sul loro operato.

Nel divenire, non resta che confidare su tutto ciò che nel nostro ordinamento può al momento costituire una garanzia per il rispetto dei diritti fondamentali degli individui, e a tal riguardo riveste particolare importanza quello statuito dal considerando 71 e dall'art. 22 del Regolamento 2016/679, che impedisce l'esclusività delle decisioni algoritmiche per le persone fisiche in un processo decisionale automatizzato.

Riferimenti bibliografici

R. Borruso (1988), *Computer e diritto*, vol. 1, Giuffrè, 1988

gli scopi più disparati all'interno dei fini del mercato unico europeo, l'Ue ha varato il Regolamento (UE) 2022/2065 – Regolamento sui servizi digitali (o *Digital Service Act*, DSA).

53. Consiglio Ue, *Regolamento sull'intelligenza artificiale: il Consiglio e il Parlamento raggiungono un accordo sulle prime regole per l'IA al mondo*, comunicato stampa, 9 dicembre 2023.

S. Civitarese Matteucci, L. Torchia (a cura di) (2016), *La tecnificazione dell'amministrazione*, in Id., "La tecnificazione", vol. IV, Firenze University Press, 2016

I. D'Elia, M. Pietrangelo (2005), *Il Codice dell'Amministrazione Digitale nel processo di semplificazione normativa: genesi e criticità*, in "Informatica e Diritto", 2005, n. 1-2

E. Fameli (1984), *Informatica e procedimenti decisionali nel diritto*, in "Informatica e diritto", 1984, n. 2

P. Ferragina, F. Luccio (2017), *Il pensiero computazionale. Dagli algoritmi al coding,* il Mulino, 2017

L. Floridi (2020), *Il verde e il blu*, Raffaello Cortina Editore, 2020

A. Gallizia, E. Maretti (1974), *Proposte metodologiche per l'uso del calcolatore elettronico come "strumento di processo" nell'operare giuridico*, in "Rivista internazionale di filosofia del diritto", 1974, n. 1

A. Malaschini (2023), *ChatGPT e simili: questioni giuridiche e implicazioni sociali*, in "Consulta online", 2023, n. 2

D. Marongiu (2022), *Algoritmo e procedimento amministrativo: una ricostruzione*, in "Giurisprudenza Italiana", 2022, n. 6

A. Masucci (2022), L'*Automazione delle decisioni amministrative algoritmiche – Fra Big Data e Machine Learning. Verso l'Algocratic Governance*, in "Diritto e processo amministrativo", 2022, n. 2

A. Masucci (1993), *L'Atto amministrativo informatico. Primi lineamenti di una ricostruzione*, Jovene, 1993

P. Passaglia (2020), *Fake news e fake democracy: una convergenza da scongiurare*, in "federalismi.it", 2020, n. 11

M. Pietrangelo, L. Nannipieri (2023), *Intelligenza artificiale e pubbliche amministrazioni, tra incertezze definitorie, usi disomogenei e giudici supplenti*, in F. Falchi, F. Giannotti, A. Monreale et al. (eds.), "Ital-IA 2023, Proceedings of the Italia Intelligenza Artificiale - Thematic Workshops", 2023

A. Trafton (2020), *Artificial intelligence yields new antibiotic*, in "MIT News", 20 February 2020

G. Zaccaria (2020), *Figure del giudicare: calcolabilità, precedenti, decisione robotica*, in "Rivista del diritto civile", 2020, n. 2

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0138 • articolo non sottoposto a peer review • pubblicato in anteprima il 2 mag. 2024

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

gennaio-aprile 2024

G. Taddei Elmi è ricercatore associato presso l'IGSG/CNR 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. Iter legislativo della proposta di regolamento sull'intelligenza artificiale - procedimento 2021/0106/COD

1.1. Risoluzione legislativa del Parlamento europeo del 13 marzo 2024 sulla 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, P9_TA(2024)0138

Il 13 marzo 2024, il Parlamento europeo (523 voti favorevoli, 46 contrari e 49 astenuti) ha adottato la posizione in prima lettura (P9_TA(2024)0138) sul testo della proposta di *Regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, presentata dalla Commissione europea il 21 aprile 2021, doc. COM(2021) 206.

Tale posizione sostituisce gli emendamenti che il Parlamento europeo aveva approvato il 14 giugno 2023 (P9_TA(2023)0236) per intraprendere successivamente i negoziati con le altre Istituzioni europee pervenuti all'accordo provvisorio del 9 dicembre 2023.

La Legge sull'IA, costituita da 180 considerando, 113 articoli e 13 allegati, sarà formalmente adottata dal Parlamento europeo nel corso della seduta plenaria di aprile 2024.

Risultano confermate tra le principali novità:

- il principio dell'alfabetizzazione in materia di IA (art. 4);
- la possibilità di utilizzare l'identificazione biometrica remota da parte delle autorità di contrasto negli spazi pubblici solo entro limiti precisi e in alcune specifiche circostanze (terrorismo, ricerca di persone scomparse, gravi crimini) (art. 5, lett. h);
- la valutazione di impatto dei sistemi di IA sui diritti fondamentali, preliminare all'immissione dei sistemi di IA nel mercato (art. 27);
- la disciplina specifica sui modelli di IA per finalità generali ovvero sistemi generali di IA utilizzabili per diversi scopi (Capo V, art. 51 e ss.), anche in relazione al regime delle sanzioni pecuniarie applicabili (art. 101);
- il consolidamento delle misure a favore dell'innovazione, in particolare a proposito degli spazi di sperimentazione normativa per l'IA (Capo VI, art. 57 e ss.)
- il rafforzamento della governance a livello dell'Unione con l'istituzione dell'Ufficio per l'IA e di un forum consultivo per fornire consulenza e competenze tecniche al Comitato europeo per l'IA nonché alla Commissione, tra l'altro coadiuvata da un gruppo di esperti scientifici indipendenti (Capo VII, art. 64 e ss.);
- il diritto alla spiegazione dei singoli processi decisionali (art. 86);
- i requisiti di trasparenza richiesti ai modelli di IA per finalità generali (cfr. art. 53 e Allegato XII).

1.2. Prospettive di adeguamento degli ordinamenti giuridici nazionali alla regolamentazione europea: designazione in Italia delle autorità nazionali competenti e del punto di contatto unico ai sensi dell'art. 70 della Legge sull'IA (AI Act)

Il 25 marzo 2024, pochi giorni dopo l'approvazione il 13 marzo 2024 dell'AI Act da parte del Parlamento europeo, il Garante per la protezione dei dati personali ha scritto al Parlamento e al Governo per rilevare la necessità di individuare le Autorità nazionali di vigilanza indipendenti e imparziali per attuare in Italia la disciplina giuridica europea sull'IA, tra queste la stessa Autorità per la protezione dei dati personali in ragione della sua competenza e delle interrelazioni tra IA e dati.

2. Iniziative legislative in Italia sull'IA

2.1. Disegno di legge n. 1066: "Norme per lo sviluppo e l'adozione di tecnologie di intelligenza artificiale", Legislatura XIX

Il 12 marzo 2024 è stato presentato il disegno di legge n. 1066 dal titolo "Norme per lo sviluppo e l'adozione di tecnologie di intelligenza artificiale". Composto da una relazione illustrativa e da sette articoli, questo disegno di legge prevede alcune misure d'intervento finalizzate a promuovere l'innovazione e le potenzialità dell'IA nella prospettiva di guidare la transizione digitale, la competitività delle imprese e la creazione di posti di lavoro di qualità e alta professionalità (art. 1 "Finalità").

Tra le principali misure è contemplata la costituzione di due fondi: (i) uno di 300 milioni di euro per ciascuno degli anni dal 2024 al 2028 destinato a sostenere la competitività tecnologica nel settore dell'IA a livello europeo e internazionale nonché a promuovere gli investimenti nella ricerca e nelle tecnologie (art. 2 "Fondo per lo sviluppo dell'intelligenza artificiale"); (ii) l'altro di 400 milioni di euro per ciascuno degli anni 2024 e 2025, allo scopo di incentivare corsi e attività di formazione per consentire ai lavoratori di acquisire nuove e maggiori competenze per affrontare l'impatto delle trasformazioni tecnologiche in atto e per adattarsi ai nuovi modelli produttivi e al mercato del lavoro (art. 3 "Istituzione del Fondo intelligenza naturale").

Si stabilisce, altresì, la realizzazione di spazi di sperimentazione normativa relativi all'uso dell'IA in numerosi settori: a) industriale e manifatturiero; b) educativo; c) agroalimentare; d) culturale e turistico; e) sanitario; f) ambientale, infrastrutturale e delle reti; g) bancario, finanziario e assicurativo; h) amministrativo; i) urbanistico; l) sicurezza nazionale; m) informatico (art. 4 "Spazi di sperimentazione normativa relativi all'impiego dell'intelligenza artificiale").

Inoltre, è garantita la trasparenza dei contenuti digitali generati dall'IA attraverso un sistema di etichettatura (*label*) e filigrana (*watermark*) che li rende riconoscibili agli utenti (art. 5 "Trasparenza dei contenuti generati da intelligenza artificiale").

Dopo aver fornito la definizione di replica digitale realizzata con l'IA il disegno di legge ne chiarisce gli usi autorizzati e non, stabilendo in caso di violazione un sistema sanzionatorio (art. 6 "Uso non autorizzato di repliche digitali realizzate con l'IA").

Infine, per favorire l'estensione dei brevetti italiani nel campo dell'IA oltre i confini nazionali è prevista l'istituzione di un apposito fondo presso il Ministero delle imprese e del made in Italy con una dotazione pari a 10 milioni di euro per l'anno 2024 che raddoppia per i successivi anni 2025 e 2026 (art. 7 "Incentivi per l'estensione dei brevetti italiani basati sull'uso dell'IA in ambito europeo ed extra europeo").

2.2. Anticipazione sulla bozza del disegno di legge sull'IA in corso di elaborazione

Come annunciato il 12 marzo 2024 dalla Presidente del Consiglio in occasione dell'evento "L'Intelligenza Artificiale per l'Italia", organizzato dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri e AgID - Agenzia per l'Italia Digitale, è in corso di elaborazione un disegno di legge che ha come obiettivo quello di stabilire dei principi e delle regole complementari a quelle del regolamento

europeo sull'IA individuando anche misure più efficaci per stimolare il tessuto produttivo e l'organismo più idoneo a svolgere le funzioni di Autorità competente sull'uso delle tecnologie basate sull'IA.

Secondo una prima bozza, non ufficiale, consultabile in Rete e datata 8 aprile 2024, il testo, intitolato "Norme di principio in materia di intelligenza artificiale", appare in linea con l'AI Act a partire dalla definizione all'art. 2 di sistema di IA, che viene ripresa totalmente (è identica).

D'altra parte, proprio per l'attuazione dell'AI Act è disposta la delega al Governo che dovrà provvedere acquisito il parere delle competenti Commissioni parlamentari e del Garante per la protezione dei dati personali (art. 22).

Tra i principi si prevede tra l'altro che l'impiego dell'IA nella pubblica amministrazione è in funzione strumentale e di supporto, restando confermata la centralità della persona umana anche in relazione ai profili di responsabilità (art. 14).

L'impiego dei sistemi di IA è, analogamente, previsto per l'organizzazione e la semplificazione del lavoro giudiziario, per la ricerca giurisprudenziale e dottrinale anche finalizzata all'individuazione di orientamenti interpretativi, per la predisposizione di bozze di provvedimenti e per ogni altro impiego funzionale e di ausilio all'attività giudiziaria (art. 15). Al comma 2 dell'art. 15 si interviene, opportunamente, disponendo, in modo espresso, che «spetta esclusivamente al magistrato la decisione sulla interpretazione della legge, sulla valutazione dei fatti e delle prove e sulla adozione di ogni provvedimento». Questa indicazione ha un valore oltre che giuridico anche scientifico-filosofico in relazione al rapporto tra IA e diritto: la macchina in quanto morfosintattica ha il grande limite semantico di non comprendere il significato del linguaggio giuridico; l'IA può compiere tutte le operazioni logiche basate su enunciati predefiniti veri, ma non è capace di stabilire la verità o la falsità di tali enunciati e non è in condizione di sussumere la fattispecie concreta nella fattispecie astratta. Questa operazione deve restare appannaggio del giurista-giudice, il quale solo ha la capacità giuridica e soggettiva di "decidere".

Riguardo alla governance, anche al fine di applicare la normativa a livello europeo, la bozza del testo in esame indica quali Autorità nazionali per l'intelligenza artificiale: l'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale (ACN) (art. 18).

Insieme ad alcune disposizioni in materia di diritto di autore (artt. 23 e 24) sono altresì previste delle modifiche al codice penale che tengono conto del possibile uso malevolo dei sistemi di IA (art. 25).

Il testo della bozza in questione si articola in cinque capi e 25 articoli rubricati come segue:

Capo I - Finalità e principi

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 nazionale
Art. 7 Criterio interpretativo e applicativo

Capo II - Disposizioni di settore

Art. 8 Accessibilità e intelligenza artificiale
Art. 9 Libera utilizzazione dei dati ai fini della ricerca e della sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario
Art. 10 Disposizioni in materia di fascicolo sanitario elettronico, sistemi di sorveglianza nel settore sanitario e governo della sanità digitale
Art. 11 Disposizioni sull'utilizzo dell'intelligenza artificiale in materia di lavoro
Art. 12 Osservatorio sull'adozione di sistemi di intelligenza artificiale nel mondo del lavoro
Art. 13 Disposizioni in materia di professioni intellettuali
Art. 14 Principi in materia di pubblica amministrazione
Art. 15 Disposizioni in materia di amministrazione della giustizia
Art. 16 Modifiche al codice di procedura civile

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. Prima puntata: dalle origini alla sistematica degli anni Settanta*

INDICE

1. Premessa

Informatica, intelligenza artificiale e robotica, sin dai lontani anni Cinquanta del secolo scorso, sono state oggetto di grande attenzione da parte di filosofi, scienziati, sociologi e anche di giuristi, che ne hanno affrontato i vari aspetti secondo le proprie competenze e visioni.

Lo scienziato "duro" si è posto la questione dei limiti della ri-produzione meccanica delle attività intellettuali umane attraverso artefatti (Seminario di Dartmouth 1956). Il filosofo ha visto nel calcolatore la grande occasione per rivisitare il cruciale problema della differenza tra uomo e macchina e tra cervello e mente. Il sociologo è stato attratto dalle conseguenze dell'uso delle macchine elettroniche nei vari ambiti della società specialmente nel lavoro. Il giurista, sia pure con iniziale forte diffidenza, si interessa al rapporto tra informatica e diritto.

Due sono i versanti considerati, uno tecnologico-applicativo (informatica giuridica) e uno squisitamente giuridico (il diritto dell'informatica). Nel primo l'artefatto appare come strumento e il mondo giuridico come oggetto, nel secondo la macchina come oggetto e il diritto come strumento.

In origine, prevalse nettamente il versante dei limiti e delle possibilità di utilizzare l'informatica nei vari ambiti giuridici ed emerse subito la grande distinzione tra programmi documentari (banche dati) e progetti decisionali (sistemi esperti). Con lo sviluppo della tecnologia il rapporto si sposta fortemente sul versante giuridico. Dalle questioni della proprietà intellettuale, alla criminalità via computer, alla

responsabilità civile e penale delle azioni dei sistemi di intelligenza artificiale, alla riservatezza dei dati e a tutte le questioni giuridiche scatenate dalla Rete Internet. Ormai oggi il diritto dell'informatica prevale nettamente sull'informatica giuridica in senso stretto intesa come documentazione e decisione.

Continua e riemerge il tema della predizione giudiziaria e della consulenza sia verso l'avvocato sia verso il giudice.

Ma andiamo per ordine e descriviamo l'itinerario della IA dalla sperimentazione tecnologica alla regolamentazione giuridica. Il percorso può essere suddiviso in stagioni di sviluppo della IA e analizzato sotto i profili del *Quid*, del *Quomodo*, del *Quid iuris* e del *Quando* della IA. Con *Quid* intendo cosa l'IA è in grado di fare; con *Quomodo* come l'IA fa quello che è in grado di fare; con *Quid iuris* quali sono le conseguenze giuridiche di quel fare e con *Quando* quale sarà il momento in cui l'IA da oggetto diventerà soggetto[1].

2. La stagione delle origini (anni Quaranta)

Nel primo periodo di uso del calcolatori elettronici non si parla di intelligenza artificiale ma di "calcolo logico delle attività cerebrali"[2], di "auto-regolazione dei sistemi artificiali e naturali in base a informazioni"[3] e di "macchine pensanti"[4].

Tutti gli scienziati si occupano di cosa possono fare gli elaboratori elettronici (*Quid*) e non si pongono la questione di come (*Quomodo*) i calcolatori fanno quello che sono in grado di fare. A maggior ragione trascurano totalmente il *Quid iuris* cioè le conseguenze giuridiche di ciò che fanno le macchine. In relazione al *Quando* forse si può cogliere *in nuce* l'idea che queste potenti macchine potranno un giorno forse uguagliare l'intelligenza umana restando, in ogni caso, sul piano dell'oggetto inconsapevole.

Gli ambiti di applicazione iniziale dei calcolatori sono soprattutto la matematica e la logica. Basti ricordare l'ABC del 1939, considerato per molti anni il primo calcolatore digitale, usato per il calcolo di sistemi di equazioni lineari, l'ENIAC del 1943, un computer *general purpose* realizzato negli Stati Uniti per calcoli matematici, il *Colossus*, progettato nel Regno Unito con il compito di decodificare i messaggi tedeschi generati dalla macchina cifratrice Lorenz SZ 40/42, basata sulla tecnologia di Enigma[5].

Negli stessi anni anche altri settori, tra cui il diritto, guardano con attenzione alle possibilità offerte dai calcolatori. Nel 1949 un esperto di antitrust, Lee Loevinger, auspica che lo studio del diritto (*Jurisprudence*), da mera attività speculativa solo interpretativa si trasformi, almeno in parte, in Jurimetrics come misurazione "scientifica" dei problemi giuridici (*Activities involving scientific investigation of legal problem*), precisando che il termine giurimetria non necessariamente deve essere considerato per indicare una disciplina scientifica ma come un programma generale da sviluppare nello studio del diritto alla stregua di biometria ed econometria[6]. Osserva inoltre che, se il diritto avesse una "struttura logica", potrebbe sfruttare le applicazioni della cibernetica e le capacità di recenti macchine, in grado di imitare il processo del pensiero attraverso numeri e simboli, con l'obbiettivo di decidere le questioni giuridiche. Ma

1. Taddei Elmi 2021.
2. Mc Culloch-Pitts 1943, pp. 115-137.
3. Wiener 1948.
4. Turing 1950.
5. *[Crittografia] La macchina enigma. Cos'era e come funzionava,* InformaticaLab, 2013..
6. Loevinger 1949, p. 483: «In the field of social control (which is law) we must at least begin to use the same approach and the same methods that have enabled us to progress toward greater knowledge and control in every other field. The greatest problem facing mankindat this midpoint of the twentieth century is the inadequacy of socio-legal methods inherited from primitive ancestors to control a society which, in all other aspects, is based upon the powerful techniques of a sophisticated science. The inescapable fact is that jurisprudence bears the same relation to a modem science of jurimetrics as astrology does to astronomy, alchemy to chemistry, or phrenology to psychology. It is based upon speculation, sup-position and superstition; it is concerned with meaningless questions; and, after more than two thousand years, jurisprudence has not yet offered a useful answer to any question or a workable technique for attacking any problem».

essendo il diritto espresso in un linguaggio vago non facilmente riducibile a numeri e simboli[7], Loevinger considera questa via ardua e più facilmente percorribile l'approccio statistico-previsionale delle decisioni basato sulla misurazione statistica dei comportamenti dei giudici[8].

La riflessione di Lovinger, tutta concentrata sulla necessità di utilizzare metodi scientifici "misuratori" (e non solo speculativi tipici a suo dire della *jurisprudence*) per affrontare molte questioni giuridiche, non pone alcuna attenzione al versante del *Quid iuris*[9].

L'ambito "giurimetrico", delineato nel 1949, verrà definito dopo alcuni anni in tre settori, l'immagazzinamento e il reperimento delle informazioni o information storage and retrieval systems (quella che sarà chiamata informatica documentaria), la previsione delle decisioni future sulla base del comportamento dei giudici (l'informatica predittiva o behavioral analysis of decisions) e la formalizzazione della conoscenza giuridica (quella che sarà chiamata informatica decisionale o dei sistemi esperti) per realizzare sistemi di consulenza e decisione giuridica[10].

Nel 1950 lo stesso Norbert Wiener, richiamando forse inconsapevolmente l'illuminismo giuridico di Beccaria, dedica al diritto un intero capitolo del suo celebre *The Human Use of Human Beings*, auspicando la formalizzazione logica delle norme e la conseguente attività giurisprudenziale sillogistica diretta a risolvere i giudizi[11]. Beccaria e Wiener, sia pure in epoche molto distanti, sono convinti che la meccanizzazione del ragionamento giuridico sia la soluzione migliore per limitare o addirittura eliminare le lentezze e le incertezze delle decisioni giuridiche. Il calcolatore sarebbe la panacea di tutti i mali della giustizia.

In riferimento alle operazioni eseguite dai calcolatori, per tutti gli anni Quaranta e i primi anni Cinquanta, non si usa l'espressione *intelligenza artificiale* bensì termini come autoregolazione (Wiener), calcolo logico-aritmetico (Turing) e misurazione statistica (Loevinger). Bisogna attendere l'agosto del 1955, quando John McCarthy (*Dartmouth College*), Marvin L. Minsky (*Harvard University*), Nathaniel Rochester (*IBM Corporation*) e Claude E. Shannon (*Bell Telephone Laboratories*), avanzano la proposta di un progetto di ricerca estivo presso il *Dartmouth College* sulla "Intelligenza Artificiale".

Secondo il "riduzionismo scientifico", preminente all'epoca, ogni aspetto dell'apprendimento e delle capacità dell'intelligenza potrebbero essere descritti in modo così preciso e dettagliato da essere simulati da una macchina.

Anche la letteratura giuridica dell'epoca, certamente influenzata dalle prospettive della IA, utilizza termini come *cybernetics*, *modern* e *simbolic logic*, *quantitative analysis*, *boolean algebra*, *machine-made justice* evitando per il momento il termine *artificial intelligence*[12].

Nell'agosto del 1956 al *Dartmouth College* di Hanover nella Contea di Grafton del New Hampshire si svolge l'auspicato *Summer Research Project* e da subito si delineano due indirizzi per modellizzare l'intelligenza umana, uno cognitivista-logico e uno connessionista-biologico[13].

7. *Ivi*, p. 471.
8. *Ivi*, p. 486.
9. *Ivi*, p. 455.
10. Baade 1963, *Foreword*.
11. Wiener 1966, pp. 128-139.
12. Baade 1963 con *ivi* numerosi articoli che passano in rassegna le applicazioni possibili del calcolatore al mondo giuridico; Bigelow 1969, dove emergono i temi di diritto dell'informatica accanto a quelli di informatica giuridica.
13. Vedi Mc Carthy-Minsky-Rochester-Shannon 1955: «We propose that a 2 month, 10 men study of artificial intelligence be carried out during the summer of 1956 at Dartmouth College in Hanover, New Hampshire. The study is to proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it. An attempt will be made to find how to make machines use language, form abstractions and concepts, solve kinds of problems now reserved for humans, and improve themselves. We think that a significant advance can be made in one or more of these problems if a carefully selected group of scientists work on it together for a summer».

Per i cognitivisti la mente/cervello non è altro che un elaboratore di simboli che codifica gli stimoli che gli arrivano dall'esterno ed elaborandoli, seguendo regole o meta-regole, arriva a una soluzione e la realizza. Il connessionismo, rifacendosi alle neuroscienze, parte dalla natura biologica dell'intelligenza e ritiene che i comportamenti intelligenti umani siano dei prodotti di combinazioni neuronali del cervello.

Il primo metodo di IA cognitiva, detto "simbolico", inizialmente prevale e prosegue per tutti gli anni Settanta e Ottanta, mentre il metodo connessionista, detto sub-simbolico, comincerà a diffondersi negli anni Novanta per divenire il più seguito e utilizzato negli anni 2000.

L'interesse dei due approcci è tutto concentrato sul come ri-produrre tecnicamente l'intelligenza biologica in un sistema elettronico, sul *Quid* e sui limiti della macchina e non sul *Quomodo* la ri-produce. La cruciale questione della soggettività delle macchine non emerge in alcun modo. I sistemi di intelligenza artificiale di questo periodo vengono considerati degli oggetti bensì intelligenti.

Anche le questioni giuridiche del *Quid iuris* che potrebbero sorgere dall'uso dei calcolatori nei vari settori della società quali il lavoro, l'informazione, la natura degli artefatti elettronici come hardware e software, la loro protezione e la contrattualistica degli stessi, non suscitano attenzione particolare.

3. La stagione "simbolica"

3.1. Il periodo della misurazione giurimetrica e della auto-regolazione "giuscibernetica" (anni Sessanta)

Negli anni Sessanta proseguono gli studi in tema di informatica documentaria, gestionale e decisionale a cui è dedicato un importante e pionieristico volume collettaneo curato da Hans Baade. La Giurimetria di Loevinger si articola in due direzione, una statistico-previsionale e una logico-formalista. Nell'opera del 1963[14] Loevinger afferma che la Giurimetria «signifies the scientific investigation of legal problems» individuandone tre aree principali l'"electronic data storage and retrieval", ossia il *Quid* informativo, la "behavioural analysis of decisions", ossia il *Quid* giurisprudenziale predittivo tipico del sociologismo e realismo giuridico anglosassone e "the use of symbolic logic", il *Quid decisionale* logico con rappresentazione formale della conoscenza giuridica che poi prevarrà nelle applicazioni in ambiente di civil law. Non si fa ancora nessun cenno ai risvolti giuridici delle applicazioni elettroniche e bisogna per questo aspettare un secondo rilevante volume collettaneo del 1969 curato da Robert Bigelow[15]. Accanto al prevalente interesse dedicato all'uso del Computer nella pratica degli uffici legali (*The Computer and the practice of Law*), come ausiliario nei procedimenti legislativi, amministrativi, fiscali e criminali (*Government and Computer*) e nella formalizzazione logica del diritto per eventuale previsione decisionale (nocciolo della *Jurimetrics*), in un capitolo dal titolo "L'avvocato e il Computer del suo cliente", dove emergono tutti i temi "giuridici" (*Quid iuris*), collegati al computer, quali la contrattualistica, gli aspetti assicurativi, e fiscali, la responsabilità per errori riguardo i dati di un giudizio (*torts*), il rilevamento di prove (*evidence*), la protezione sotto il profilo della proprietà intellettuale di hardware e software, la privacy connessa alle banche dati, la violazione di copyright e le questioni bancarie .

L'irrompere della macchina nelle attività tipiche dell'uomo stimola, come già detto, specialmente i filosofi in generale ma in particolare i filosofi del diritto. Le ragioni sono almeno tre: come sociologi del diritto sono attratti dai risvolti sul lavoro, come scienziati del diritto vedono nel calcolatore uno strumento per rivisitare in modo rigoroso i procedimenti logici del ragionamento giuridico e come filosofi in generale si pongono domande sulla natura delle macchine intelligenti e sulla eticità del loro uso.

Mario Losano si occupa in uno scritto del 1969[16] della Giurimetria e dei suoi primi ambiti applicativi, criticandone il carattere esclusivamente pratico. Ne teorizza il superamento verso la Giuscibernetica,

14. Loevinger 1963.

15. Bigelow 1969, dove emergono i temi di diritto dell'informatica accanto a quelli di informatica giuridica. Da segnalare una terza edizione del 1981 sempre curata da Robert Bigelow, che sviluppa fortemente gli aspetti di diritto dell'informatica nei capp. V *Contracts for Computers and Computer Services* e VI *Some Legal Aspects of Computer Usage*.

16. Losano 1969.

vera disciplina scientifica, indirizzata verso quattro approcci distribuiti fra due componenti, una più teorica, la modellistica giuridica, e l'altra più empirica, l'informatica giuridica; la prima dovrebbe studiare il sistema giuridico come sottosistema del sistema sociale (primo approccio) e poi la sua struttura dinamica (secondo approccio); la seconda componente avrebbe con oggetto il sistema giuridico come sistema di norme – analisi del linguaggio giuridico e logica giuridica (terzo approccio) – e l'utilizzazione pratica degli altri approcci (quarto approccio). La critica di Losano mi pare eccessiva dato che Loevinger, nel suo primissimo scritto, considera il "diritto" come una forma di controllo sociale[17] da studiare con metodi scientifici e nel volume del 1963 descrive la *Jurimetrics* con tre aree[18] tra cui emerge l'uso della logica simbolica per analisi del sistema e delle norme.

Nella riflessione di Losano non appaiono cenni agli aspetti di *Quid iuris* e men che meno a futurologiche capacità soggettive delle macchine cibernetiche.

Vittorio Frosini nello stesso anno pubblica *Cibernetica, diritto e società*, libro ormai entrato tra i classici della informatica giuridica dove come filosofo e sociologo spazia su molti temi del rapporto tra macchina e uomo[19]. Tra cui veramente pionieristiche sono le riflessioni sulla "coscienza artificiale" del robot inteso anche come soggetto morale.

3.2. Il periodo "sistematico": Informatica giuridica e Diritto dell'informatica (anni Settanta)

Con gli anni Settanta inizia un percorso parallelo tra informatica giuridica[20] e diritto dell'informatica[21]. Gli studi scientifici, pur trattando insieme i due temi[22] li distinguono abbastanza nettamente e tentano una sistematica all'interno della informatica giuridica (IG) tra le varie applicazioni con risultati nella maggior parte insoddisfacenti[23].

Lo sforzo sistematico, a mio avviso, più fecondo è quello di Andreas Tschudi del 1977[24]. Affronta la questione disciplinare della informatica giuridica chiedendosi *Warum ist die Rechtsinformatik eine selbstandige wisseschaftliche Disziplin?* e *Wo befindet sich Rechtsinformatik im System der Wissenschaften?* Dopo aver analizzato i vari criteri, che possono essere utilizzati per stabilire l'unitarietà di una disciplina scientifica, come il linguaggio, il metodo e l'oggetto, opta per quest'ultimo ponendo però una interessante distinzione tra "oggetto dell'esperienza" (*Erfahrungsobject* ossia l'ambito applicativo concreto (*Gegenstandbereich*) e "oggetto della conoscenza" (*Erkenntnisobjekt*) ossia l'ambito problematico (*Problembereich*).

Sulla base dell'analisi dello studioso svizzero emerge che l'IG non è una disciplina unitaria ma che vi sono tante IG quanti sono gli oggetti della conoscenza e che queste IG sono in ogni caso interdiscipline sotto il profilo dell'oggetto dell'esperienza[25].

17. Loevinger 1949, p. 483.
18. Baade 1963, *Foreword*.
19. Frosini 1968 (edizioni accresciute successive nel 1973, 1977, 1978 e 1983), ora edito in formato digitale nella Collana "La memoria del diritto", Roma TrE-Press, 2023.
20. Negli anni Settanta si verifica un boom di manuali e scritti generali di Informatica Giuridica: Steinmüller 1970, p. 127 e ss.; Tapper 1973; Chouraqui 1974; De Santis Garcia 1976; Haft 1977; Reisinger 1977.
21. 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, che dalla prima edizione del 1978, edita da Longman Group Limited, Longman House, Burnt Mill, Harlow, (UK), non si intitolano più *Computers and Law* ma *Computer Law* (il diritto dei computer) e sono dedicati esclusivamente al *Quid iuris* (le successive edizioni sono del 1982, 1983, 1989, 1990).
22. Mackaay 1971, pp. 12-15; Tapper 1973; Bing-Harvold 1977 (Rassegna completa e aggiornata dei sistemi informatico-giuridici sia informativi sia decisionali).
23. Steinmüller 1970; Fiedler 1974, pp. 198-205; Haft 1977; Reisinger 1977; Tschudi 1977. Per una analisi degli approcci sistematici rinvio ad alcuni miei contributi: Taddei Elmi 1990, pp. 3-19 e pp. 33-58 e più recentemente Taddei Elmi 2006, pp. 5-19.
24. Tschudi 1977.
25. Taddei Elmi 2010, pp.187-193.

Che l'IG sia totalmente distinta, sia logicamente sia epistemologicamente, dal diritto dell'informatica (DI) era stato da me sottolineato sin dal 1972[26], mentre alla conclusione che l'IG non sia una disciplina unitaria ma un insieme di discipline connotate dal proprio oggetto della conoscenza sono giunto sulla base della mia lunga esperienza di ricercatore[27].

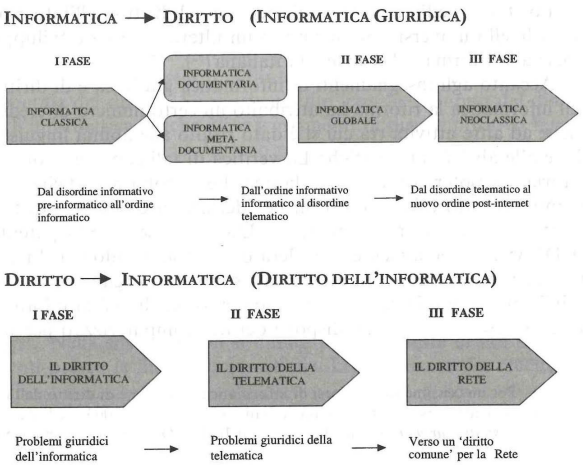
Riporto un paio di tabelle che danno il quadro delle applicazioni informatico-giuridiche e il rapporto tra IG e DI.

Schema dell'informatica giuridica

Informatica giuridica	*Oggetto esperienza primario (P) e secondario (S)*	*Oggetto conoscenza*
Informatica giuridica documentaria	Elettronica (P) Documentazione (P) Documentazione giuridica (S)	informatizzazione Documentazione giuridica
Informatica giuridica cognitiva	Elettronica (P) Scienza della conoscenza (P) Conoscenza giuridica (S)	Informatizzazione della conoscenza giuridica
Informatica giuridica gestionale	Elettronica (P) Gestione dell'ufficio (P) Organizzazione ufficio del giurista (S)	Informatizzazione dell'ufficio legale
Informatica giuridica redazionale	Elettronica (P) Gestione del documento (P) Gestione del documento giuridico (S)	Informatizzazione redazione documento giuridico
Informatica giuridica didattica	Elettronica (P) Didattica (P) Didattica giuridica (S)	Informatizzazione della didattica giuridica

La mia opinione di allora e di oggi è che il DI non ha nulla a che vedere con l'IG se non per alcuni aspetti border line quali ad esempio la firma digitale, il PCT, il diritto di autore in relazione a opere contenute in banche dati, dove i due versanti si incontrano in cima a un crinale.

Schema dei rapporti tra informatica e diritto



[Fine della prima parte. La seconda parte sarà pubblicata in un prossimo aggiornamento della rubrica].

26. Taddei Elmi 1972, p. 666 ss.

27. Taddei Elmi 2006, pp. 13 e ss.; Taddei Elmi 2016, pp. 18-26.

2. Saggi e volumi

V. Cuocci, F.P. Lops, C. Motti (a cura di), *La Governance nell'era digitale* (Atti della Summer school 2022), Università degli studi di Foggia, Dipartimento di Giurisprudenza, Cacucci Editore, Bari, 2023

Il volume è articolato in quattro parti: Parte I: Dati, piattaforme e "sistemi intelligenti", Parte II: Imprese, mercati e transizione digitale, Parte III: Le professioni intellettuali nel "mondo nuovo", Parte IV: Governare l'innovazione: etica, regole, standard. Si segnala nella Parte I: A. Gentili, *Informazione e consenso nella rete: una breve introduzione*; M.C. Cavallaro, *Amministrazione pubblica e sistemi di intelligenza artificiale* e G. Taddei Elmi, *L'IA tra oggetto e soggetto: dalle "cose" alle "persone". Dall'oggetto al soggetto ontologico attraverso il soggetto ascritticio*; nella Parte IV: G. Di Rosa, *L'automazione intelligente tra conformazione normativa e discipline innovative*; M. Granieri, *Uno sguardo comparativo sulle fonti normative in materia di intelligenza artificiale;* P. Buono, *Intelligenza artificiale ed etica*; P. Annicchino, *Le tecnologie emergenti tra algoretica e regolazione* e A. Punzi, *Governance condivisa, La regolazione dei contenuti in rete oltre la separazione tra pubblico e privato*.

E. Bellisario, G. Cassano (a cura di), *Intelligenza artificiale per la pubblica amministrazione*, Pacini Giuridica, Pisa, 2023

Il volume contiene 23 contributi che analizzano, sotto vari profili, il tema dell'IA in relazione alla pubblica amministrazione e al procedimento amministrativo algoritmico. Qui di seguito si riportano i titoli e i rispettivi autori: 1 – *Introduzione all'intelligenza artificiale* (Roberta Raimondo); 2 – *Intelligenza artificiale e amministrazione digitale: possibili sviluppi della legislazione italiana* (Enrico De Giovanni); 3 – *Il quadro normativo vigente in materia di IA nella pubblica amministrazione (CAD, GDPR, IA ACT)* (Silvia Cal); 4 – *L'istruttoria algoritmica* (Davide Mula); 5 – *La decisione amministrativa algoritmica tra efficienza e garanzie* (Antonino Mazza Laboccetta); 6 – *La partecipazione procedimentale* (Tommaso Cocchi); 7 – *Legalità algoritmica e vizi procedimentali* (Ernesto Belisario e Francesca Ricciulli); 8 – *Discrezionalità algoritmica e sindacato del giudice amministrativo* (Anna Corrado); 9 – *Il lavoro umano nella pubblica amministrazione algoritmica* (Andrea Tatafiore); 10 – *Trattamento dei dati personali e processo decisionale automatizzato nella PA* (Giuseppe D'Acquisto); 11 – *La trasparenza amministrativa e gli algoritmi* (Enrico Carloni); 12 – *Dati di addestramento, intelligenza artificiale e pubblica amministrazione* (Eugenio Prosperetti); 13 – *Cybersecurity e Intelligenza artificiale: tra nuove sfide e profili di criticità* (Stefano Aterno); 14 – *Il procurement di soluzioni di IA* (Elio Guarnaccia e Giulia Campo); 15 – *Amministrazione algoritmica e responsabilità* (Giuseppe Maria Marsico); 16 – *L'uso di soluzioni di riconoscimento facciale per la sicurezza* (Riccardo Lanzo); 17 – *L'uso di soluzioni IA in sanità* (Michele Iaselli); 18 – *Algoritmi e appalti pubblici* (Elio Guarnaccia); 19 – *Apprendimento automatico e interpretazione delle norme* (Ludovico Anselmi); 20 – *Non solo chatbot: IA e comunicazione con i cittadini* (Angela Creta); 21 – *Intelligenza Artificiale per controlli amministrativi e rilevamento delle frodi* (Fabrizio Paonessa); 22 – *Amministrazione della giustizia e intelligenza artificiale* (Antonella Ciriello); 23 – *L'IA per il monitoraggio delle politiche pubbliche* (Andrea Del Forno).

N. Cristianini, *Machina Sapiens. L'algoritmo che ci ha rubato il segreto della conoscenza*, il Mulino, 2024

Le macchine possono pensare? Partendo dal noto quesito posto dal matematico britannico Alan M. Turing nel 1950, l'Autore spiega perché oggi è possibile affermare che le macchine rivelano una capacità di pensare e conversare in modo umano, imparando dai propri errori, fino a preconizzare nel prossimo futuro anche prestazioni super-umane, tenuto conto delle recente evoluzione tecnica e di esempi, come GPT-4, che rappresentano i primi passi per sistemi sempre più intelligenti in generale e l'inizio dell'era di *Machina sapiens*. Alla fine del volume è presente un glossario informale che definisce in

modo chiaro diversi termini e la bibliografia per la comprensione e l'approfondimento dei principali temi trattati.

R. Di Carmelo, *L'era degli algoritmi e la sua incidenza nell'ambito della certezza del diritto: un connubio sospetto*, in "Il lavoro nella giurisprudenza", 2024, n. 1

L'Autore si sofferma sulla giustizia predittiva e l'avvento della dimensione tecnologica nel diritto mettendo in guardia da soluzioni illusorie e indebite semplificazioni volte ad "accantonare" la persona fisica. Nel lavoro privato e pubblico si intravede il rischio di una «collusione algoritmica, declinata a favore dei desiderata del datore di lavoro» nonché la contrazione dell'occupazione in termini quantitativi e qualitativi, insieme a possibili discriminazioni non solo nel corso del rapporto di lavoro, ma nella procedura di selezione del lavoratore. In tale contesto emerge, ad esempio, l'importanza del controllo sul codice sorgente dell'algoritmo al fine di verificarne la reale trasparenza, imparzialità e terzietà nonché in generale la necessità di una rilettura complessiva delle tutele.

G. Finocchiaro, *Intelligenza artificiale. Quali regole?*, il Mulino, Bologna, 2024

Il volume, diviso in quattro parti, è un valido strumento di conoscenza delle principali problematiche connesse all'IA. Dopo l'illustrazione, nella prima parte ("Lo scenario"), del contesto culturale legato all'IA e della questione della soggettività dell'IA, l'Autrice si sofferma nella seconda parte ("Le scelte regolatorie") sui modelli regolatori, occupandosi poi nella terza parte ("Focus su alcune questioni specifiche") su alcuni aspetti particolare legali al tema dell'IA: i dati, la responsabilità e il diritto d'autore. Infine nella quarta parte ("Il contesto internazionale") si affrontano gli approcci regolatori in USA, Cina e Unione europea evidenziando alcune criticità dell'AI Act.

C. Attività internazionali

1. Convenzione quadro sull'intelligenza artificiale, i diritti umani e lo Stato di diritto, Consiglio d'Europa

Il 14 marzo 2024 la Segretaria Generale del Consiglio d'Europa, Marija Pejčinović Burić, ha annunciato la conclusione di una *Convenzione quadro sull'IA, i diritti umani, la democrazia e lo Stato di diritto*. In particolare, elaborata dal Comitato sull'intelligenza artificiale (CAI), costituito dai rappresentanti dei 46 Stati membri del Consiglio d'Europa, designati dai rispettivi governi, la Convenzione sarà sottoposta nel prossimo mese di maggio al Comitato dei Ministri per l'adozione e successivamente alla sottoscrizione.

2. Dichiarazione di Trento sull'Intelligenza artificiale

Il 15 marzo 2024, sotto la Presidenza italiana, i Ministri del G7, riunitisi a Trento, hanno adottato la Dichiarazione che promuove lo sviluppo e l'utilizzo etico dell'IA nel settore pubblico.

In tale occasione è stato riconosciuto il ruolo guida del G7 nella promozione della cooperazione internazionale per la governance globale dell'IA e l'impegno della Presidenza italiana del G7 a continuare il processo Hiroshima AI lanciato nel 2023 durante la Presidenza giapponese del G7.

Tale accordo segue la riunione *Hiroshima AI Process: The Way Ahead* e la definizione, il 30 ottobre 2023, dei principi guida internazionali *Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI system* e il codice di condotta volontario per gli sviluppatori di sistemi di IA avanzati *Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems*.

3. Iniziative e approcci regolatori nel Regno Unito

3.1. Artificial Intelligence (Regulation) Bill [HL]

Nel Regno Unito sono in corso diverse iniziative in tema di IA in attesa dell'elaborazione di un'apposita disciplina giuridica, attualmente ritenuta prematura e un possibile ostacolo allo sviluppo tecnologico dell'IA. A fronte di tale approccio si segnala in ogni caso il testo "Artificial Intelligence (Regulation) Bill [HL]", presentato il 22 novembre 2023 davanti alla House of Lords che individua in nove sezioni alcuni punti per indirizzare la futura regolamentazione sull'IA e detta alcuni importanti principi. In particolare:

- la prima sezione (*The AI Authority*) prevede l'istituzione di una autorità, *AI Authority*, competente, tra l'altro, per la individuazione e valutazione dei rischi dei sistemi di IA;
- la seconda sezione (*Regulatory principles*) sancisce alcuni principi fondamentali della regolamentazione in questione ai quali l'*AI Authority* deve fare riferimento, quali (i) sicurezza e robustezza, (ii) trasparenza e spiegabilità, (iii) equità, (iv) accountability e governance, (v) possibilità di agire in giudizio. A questi si aggiungono i principi ai quali devono conformarsi i produttori, fornitori e distributori di sistemi di IA: (a) trasparenza, (b) osservanza della normativa vigente (compresa la disciplina giuridica in materia di protezione dei dati e di proprietà intellettuale);
- la terza sezione (*Regulatory sandboxes*) riguarda gli spazi di sperimentazione;
- la quarta sezione (*AI responsible officers*) stabilisce il principio secondo il quale i produttori, fornitori e sviluppatori che installano o utilizzano l'IA devono designare un responsabile (*AI officer*) con il compito di assicurare l'uso sicuro, etico, non discriminatorio dell'IA anche in relazione ai dati;
- la quinta sezione (*Transparency, IP obligations and labelling*) prevede tra l'altro l'obbligo in capo a coloro che sono coinvolti nell'addestramento dell'IA di fornire all'*AI Authority* le informazioni relative ai dati e alla proprietà intellettuale nonché di dare ai consumatori chiare avvertenze riguardo alla salute;
- la sesta sezione (*Public engagement*) promuove il coinvolgimento della collettività al fine di assicurare la diffusa consapevolezza dei benefici e dei rischi dell'IA;
- la settima sezione (*Interpretation*) precisa la definizione legislativa del termine IA che comprende anche quella generativa;
- la ottava sezione (*Regulations*) individua nel testo legislativo lo strumento per introdurre la regolamentazione in materia di IA che dovrà anche prevedere un regime sanzionatorio;
- la nona e ultima sezione precisa l'ambito di applicazione della regolamentazione in questione (Inghilterra, Galles, Scozia e Irlanda del Nord), la sua entrata in vigore (il giorno successivo alla sua approvazione) e denominazione "Artificial Intelligence (Regulation) Act 2024".

3.2. Generative AI framework for HM Government

Sempre nel Regno Unito, il 18 gennaio 2024 è stata pubblicata la guida *Generative AI framework for HM Government* per l'utilizzo sicuro dell'IA generativa, diretta ai dipendenti pubblici e alle persone che lavorano nelle organizzazioni governative. Elaborata dal *Central Digital and Data Office*, con il supporto di numerosi autorevoli soggetti provenienti anche dal mondo della ricerca e dell'industria, la guida individua tra l'altro dieci principi sull'uso dell'IA generativa a livello governativo e nel settore pubblico fornendo anche importanti spiegazioni e chiarimenti.

D. Eventi, seminari, convegni, notizie

- Incontri sull'intelligenza artificiale (ordine Avvocati Napoli)

Organizzato dal Cnr-Iriss e dall'Ordine degli Avvocati di Napoli, il progetto si articola in una serie di incontri (14 e 21 marzo, 11 e 18 aprile, 9, 16 e 23 maggio 2024) finalizzati a rendere accessibile un'informazione "tecnica" sulle applicazioni e l'impatto dell'IA nonché a verificare le relazioni con le attività realizzate con metodi tradizionali. Gli approfondimenti programmati riguardano vari ambiti: modelli

di linguaggio, etica, privacy, diritti fondamentali, giustizia predittiva, stereotipi di genere, gestione del rischio, impatto su procedure legislative, amministrative, giudiziarie.
Il programma degli incontri è consultabile nella sezione eventi del sito web dell'IRISS-CNR.

– L'Intelligenza Artificiale per l'Italia (Convegno Dipartimento per la trasformazione digitale e AgID)

Il 12 marzo 2024 si è tenuto il convegno organizzato dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri e AgID - Agenzia per l'Italia Digitale. Tra i numerosi e autorevoli interventi sono stati illustrati alcuni punti centrali della strategia nazionale in tema di IA e le prospettive in termini di investimenti per la ricerca e pubblica amministrazione.

Il convegno è visibile sulla piattaforma YouTube (prima parte – seconda parte)

Riferimenti bibliografici

H. Baade (ed.) (1963), *Jurimetrics*, Basic Books, 1963

E. Bellisario, G. Cassano (a cura di) (2023), *Intelligenza artificiale per la pubblica amministrazione*, Pacini Giuridica, 2023

R.P. Bigelow (ed.) (1969), *Computers and the Law*, Commerce Clearing House, II ed., 1969

J. Bing, T. Harvold (1977), *Legal Decisions and Information Systems*, Universitetsfolrlaget, 1977

A. Chouraqui (1974), *L'informatique au service du droit*, P.U.F., 1974

N. Cristianini, *Machina Sapiens. L'algoritmo che ci ha rubato il segreto della conoscenza*, il Mulino, 2024

V. Cuocci, F.P. Lops, C. Motti (a cura di) (2023), *La Governance nell'era digitale* (Atti della Summer school 2022), Università degli studi di Foggia, Dipartimento di Giurisprudenza, Cacucci Editore, 2023

D. De Santis Garcia (1976), *Introduçao à informática jurídica*, J. Bushatski Editora da Universidade de São Paulo, 1976

R. Di Carmelo (2024), *L'era degli algoritmi e la sua incidenza nell'ambito della certezza del diritto: un connubio sospetto*, in "Il lavoro nella giurisprudenza", 2024, n. 1

H. Fiedler (1974), *Grundprobleme der Juristischen Informatik*, in "Datenverarbeitung im Recht", vol. 3, 1974, n. 3-4

G. Finocchiaro (2024), *Intelligenza artificiale. Quali regole?*, il Mulino, 2024

V. Frosini (1968), *Cibernetica, diritto e società*, Ed. Comunità, 1968

F. Haft (1977), *Einführung in die Rechtsinformatik*, Verlag Karl Alber, 1977

L. Loevinger (1963), *The Metodology of Legal Inquiry*, in H. Baade (ed.), "Jurimetrics", Basic Books, 1963

L. Loevinger (1949), *Jurimetrics - Next step forward*, in "Minnesota Law Review", vol. 33, 1949, n. 5

M.G. Losano (1969), *Giuscibernetica. Macchine modelli cibernetici nel diritto*, Piccola Biblioteca Einaudi, 1969

E. Mackaay (1971), *Jurimétrie, informatique juridique, droit de l'informatique,* in "Revue juridique Themis, Bibliothèque National du Québec", 1971, n. 1

J. Mc Carthy, M.L. Minsky, N. Rochester, C.F. Shannon (1955), *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, 1955

W.S. Mc Culloch, W.A. Pitts (1943), *Logical Calculus of Ideas Immanent in Nervous Activity*, in "Bullettin of Mathematical Biophisics", 1943, n. 5

L. Reisinger (1977), *Rechtsinformatik*, Walter de Gruyter, 1977

W. Steinmüller (1970), *EDW und Recht. Einführung in die Rechtsinformatik*, in "Juristisches Arbeitsblätte", 1970, n. 6

G. Taddei Elmi (2021), *Il Quid, il Quomodo e il Quid iuris dell'IA. Una riflessione a partire dal volume "Diritto e tecnologie informatiche",* in "Rivista italiana di informatica e diritto", 2021, n. 2

G. Taddei Elmi (a cura di) (2016), *Corso di informatica giuridica*, IV ed., Simone, 2016

G. Taddei Elmi (2010), *Corso di informatica giuridica*, III ed., Simone, 2010

G. Taddei Elmi (a cura di) (2006), *Abilità informatiche per il diritto*, Giuffrè, 2006

G. Taddei Elmi (1990), *Dimensioni dell'informatica giuridica. Dall'informatica 'intelligente' all'informatica 'cosciente'?*, Liguori Editore, 1990

G. Taddei Elmi (1972), *Per un'introduzione al diritto dell'informatica. L'ordinamento giuridico francese e l'informatica*, in "Bollettino d'informatica generale e applicata al diritto", 1972, n. 3-4

C. Tapper (1973), *Computers and Law*, Weidenfeld and Nicholson, 1973

A Tschudi (1977), *Rechtsinformatik*, Schultess Polygraphischer Verlag, 1977

A. Turing (1950), *Computing Machinery and Intelligence,* in "Mind", vol. LIX, 1950, n. 236

N. Wiener (1966), *Introduzione alla cibernetica. L'uso umano degli esseri umani* (tit. orig. *The Human Use of Human Beings*, Houghton Mifflin Company, 1950), Boringhieri, 1966

N. Wiener (1948), *Cybernetics. The Control and Communication in the Animal and the Machine*, Wiley, 1948

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0134 • articolo non sottoposto a peer review • pubblicato in anteprima il 1 mar. 2024

Fernando H. Llano Alonso

Presentación del artículo "Vittorio Frosini y los nuevos derechos de la sociedad tecnológica" de Antonio-Enrique Pérez Luño

***Ri*Leggiamoli**

Antonio-Enrique Pérez Luño

Vittorio Frosini y los nuevos derechos de la sociedad tecnológica

Informatica e diritto, 1992, n. 1-2, pp. 101-112

L'Autore è decano della facoltà di Giurisprudenza dell'Università di Siviglia

Transcurrido más de medio siglo del inicio de su carrera académica, el *cursus honorum* de Antonio Enrique Pérez Luño está jalonado por más de medio millar de publicaciones que le han servido para ser reconocido como uno de los grandes maestros de la doctrina iusfilosófica española contemporánea.

Su producción científica podría clasificarse en tres grandes bloques temáticos agrupados en torno a los siguientes descriptores: la teoría del derecho, los derechos humanos (bloque del que forman parte, como subcategoría, sus trabajos sobre nuevas tecnologías, informática y derecho), y la historia del pensamiento jurídico.

A propósito de ese apartado temático autónomo, el que concierne tanto al estudio del impacto de la informática y las nuevas tecnologías en el mundo del derecho, como del poder de transformación social que tienen determinados productos tecnológicos, en particular los ordenadores, puede considerarse al Prof. Pérez Luño como el pionero en España sobre esta temática.

Sus primeros estudios en torno a esta cuestión datan de principios de la década de los años '70 del pasado siglo, y se han prolongado hasta sus últimos trabajos, en los que ha abordado a fondo las grandes dicotomías ético-jurídicas que entrañan las tecnologías emergentes, como la inteligencia artificial, y se ha pronunciado contrario a la sustitución del paradigma humanista e ilustrado de la modernidad por el paradigma posthumanista que propone el transhumanismo tecnológico.

A lo largo de esas cinco décadas que marcan el itinerario intelectual e iusfilosófico de Pérez Luño, destacan tres monografías de referencia para los estudiosos de la iuscibernética y la informática jurídica: *Cibernética, informática y derecho* (1973); *Manual de informática y derecho* (1996); *Ciberciudadanía o ciudadanía.com* (2004).

El descubrimiento por parte de Pérez Luño de la informática jurídica y la iuscibernética se produce de la mano de sus maestros italianos, Vittorio Frosini y Mario Losano, a quienes conoce con ocasión de un seminario organizado en 1968 por el Rector del Colegio de España en Bolonia Evelio Verdera y Tuells, institución de la que en ese momento era estudiante de doctorado Pérez Luño (cuya tesis, por cierto, fue dirigida por Guido Fassò). Ambos maestros italianos habían sido pioneros en el estudio de la informática jurídica y la cibernética aplicada al derecho.

En el momento en que Antonio Pérez Luño conoce a Losano y Frosini, ambos maestros iusfilósofos ya habían publicado ensayos sobre esta materia tan novedosos como relevantes. En este sentido, Mario Losano había publicado, en el año 1968, dos artículos en la revista *Law and Computers Technology* sobre derecho y tecnología e informática jurídica, y un capítulo de libro titulado "Giuscibernética", que solo un año más tarde aparecería en forma de monografía.

Por su parte, ese mismo año, Vittorio Frosini había publicado el libro *Cibernética, diritto e società*. Para Pérez Luño se trata de un texto avanzado a su época, en la medida que en él se vislumbra el control de la sociedad y la vigilancia de la vida privada de los individuos por medio de la tecnología y los sistemas informáticos.

El texto de Antonio Pérez Luño que he elegido para este número dedicado a Vittorio Frosini es, a mi juicio, uno de los que mejor extracta la influencia de la "consciencia tecnológica" del iusfilósofo italiano en su discípulo español, sobre todo en lo concerniente a los nuevos derechos humanos en la sociedad tecnológica domeñada por la inteligencia artificial. Advierte Pérez Luño, que en este contexto artificial, existe un riesgo evidente de que los valores y los derechos humanos, en cuanto producto de la conciencia o ética autónoma de la persona, sean suplantados por una conciencia externa o heterónoma, que expresa la artificialidad del pensamiento tecnológico.

Frosini y Pérez Luño comparten una común visión generacional de los derechos humanos. En

el catálogo de derechos y libertades de tercera generación, que tienen a la humanidad como principal titular, y la solidaridad como principio-guía, destaca el derecho a la libertad informática, una modalidad de libertad personal reconocida a los ciudadanos que tiende a proteger su "identidad informática".

Para el ejercicio del derecho a la libertad informática, señala Frosini, es preciso que los ciudadanos puedan conocer y acceder a los datos personales e informaciones que les afectan y que se almacenan en archivos digitales y bases de datos. Así pues, al tradicional derecho de *habeas corpus* como garantía de la libertad física o de movimiento de la persona, le corresponde en la sociedad tecnológica el derecho de *habeas data*, un cauce procesal para la salvaguarda de la libertad de la persona en la esfera informática.

Uno de los aspectos más destacables de la teoría de los derechos humanos en el pensamiento de Vittorio Frosini es, a juicio de Pérez Luño, su concepción heteropoiética de los mismos. En efecto, frente a la concepción autopoiética, intrasistemática y autorreferencial que de los mismos tienen autores como Niklas Luhmann y Gunther Teubner, la teoría de Frosini representa una visión rehabilitadora de los presupuestos extrasistemáticos, abiertos y heteropoiéticos de tales derechos.

En suma, la principal aportación de Frosini a la doctrina de los derechos humanos consiste, según Pérez Luño, en su apertura al estimulante mundo de la ciencia y la tecnología. En este sentido, el mérito de Frosini estriba, sobre todo, en haber puesto de manifiesto que la teoría de los derechos humanos debía responder a los retos de la sociedad tecnológica contemporánea. Por eso, concluye Pérez Luño, no solamente los discípulos y colaboradores de Frosini, sino todos aquellos estudiosos de los derechos humanos desde una conciencia tecnológica, son deudores suyos en términos científicos e iusfilosóficos.

Vittorio Frosini y los nuevos derechos de la sociedad tecnológica

ANTONIO-ENRIQUE PEREZ LUÑO

1. VITTORIO FROSINI: UN ANTICIPADOR DE LA FILOSOFÍA DEL DERECHO DEL PORVENIR

Vittorio Frosini es un de las más relevantes figuras del prestigioso grupo de filósofos del Derecho que han enseñado en Italia en el periodo que abarca desde la postguerra a la actualidad. Herederos inmediatos de las versiones jurídicas del idealismo, el neokantismo, el positivismo y el historicismo, los filósofos del Derecho italianos iniciaron, al promediar nuestro siglo, un ambicioso movimiento de renovación de la cultura jurídica de amplia y profunda influencia. El nuevo positivismo jurídico de orientación analítica que surge en torno al estímulo intelectual de Norberto Bobbio, la formación de una Escuela italiana de Sociología del Derecho promovida por Renato Treves, o el decisivo impulso que para la historiografía filosóficojurídica supone la obra de Guido Fassò, constituyen aspectos insoslayables de este importante capítulo de la historia de la Filosofía del Derecho contemporánea.

Frosini coincide temporalmente con esa pléyade doctrinal, pero no mentalmente. Los presupuestos y las inquietudes de su pensamiento le sitúan como un adelantado del siglo venidero. El plano teórico de su reflexión está en lo radical de su propósito anticipando los temas de lo que puede ser la Filosofía del Derecho del porvenir. Esta condición suya le lleva a una vida intelectual inquieta, dinámica, más preocupada de adivinar los rumbos futuros de la reflexión iusfilosófica que a explicar sus problemas pasados[1].

[1] Me he ocupado anteriormente de distintos aspectos del pensamiento y la obra de Vittorio Frosini en mis trabajos: *Tradizione e novità ne «La struttura del diritto» di Vittorio Frosini*, en «Rivista Intemazionale di Filosofia del Diritto», 1973, pp. 315 ss.; *Introducción al pensamientofilosófico jurídico de Vittorio Frosini*, Estudio Preliminar a la trad. cast. del vol. de V. Frosini, *La estructura del Derecho*, Publicaciones del Real Colegio de España, Bolonia, 1974, pp. 7 ss.; así como en el *Prólogo*, a la trad. cast. del vol. de V. Frosini, *Cibernética, derecho y sociedad*, Tecnos, Madrid, 1982, pp. 11 ss.

Como todo pensador esencialmente crítico su obra arranca y se explicita en tensión polémica con dos de las más influyentes interpretaciones del Derecho de nuestro tiempo: el idealismo y el kelsenianismo. El contexto en el que se inicia la vocación filosóficojurídica de Frosini se halla impregnado de idealismo. A esa corriente pertenecieron algunos de sus maestros, cuyos nombres se inscriben entre los más representativos del neoidealismo italiano: Giovanni Gentile, Guido Calogero, Francesco Collotti, Angelo Ermanno Cammarata, Orazio Condorelli... Es cierto que para Frosini el Derecho será definido como «morfologia della prassi», pero esa praxis no tendrá un sentido ideal y abstracto, sino que será fruto de un proceso de estructuración en formas definidas por la acción social. Además al apriorismo de la concepción idealista del Derecho, opondrá Frosini – y a ello no será ajeno el influjo intelectual de Giuseppe Capograssi – el carácter de experiencia común del Derecho, como realidad propia de las formas concretas de vida social[2].

De Kelsen, dirá Frosini, que puede repetirse respecto a él lo que afirmaba Hegel con relación a Spinoza: que era necesario spinozieren para poder *philosopllieren*. El sistema de Spinoza representó un momento clave en la historia del pensamiento europeo, que, por ello mismo, debía ser superado. Según Vittorio Frosini, Kelsen se asemeja a Spinoza: en ambos se dá idéntica exigencia especulativa de un absoluto monismo, en función del cual Dios se hace naturaleza en Spinoza, y el Estado se hace Derecho en Kelsen. Al *ordo rerum* y al *ordo idearum* del primero, le corresponde el paralelismo entre los hechos y las normas propugnado por el segundo. Se dá incluso entre ambos la curiosa mezcla entre el reconocimiento del derecho de la fuerza, entendido como el único auténtico Derecho natural, y la enérgica afirmación del deber de tolerancia cívica de las filosofías y de las creencias (ideologías para Kelsen) contrastantes. Frente al spinozismo jurídico de Kelsen, frente a su rigurosa concatenación de normas, y la coherencia lógica de su pensamiento, frente a ese «espíritu sistemático» despectivo de la realidad y de las pasiones e ilusiones humanas, opone Frosini las exigencias fácticas y axiológicas de la experiencia jurídica. Las objeciones avanzadas por Vico respecto al spinozismo, en nombre de la humanidad que lucha trabajosamente por construir su historia en función de la imagen de una humanidad mejor, son retomadas por Frosini para reafirmar los valores que fundamentan e inspiran la experiencia histórica del Derecho[3].

[2] Cfr. sobre ello, V. Frosini, *La estructura del Derecho*, cit., pp. 45 ss.; id., *L'idealismo giuridico italiano*, Giuffrè, Milano, 1978, passim; id., *Saggi su Kelsen e Capograssi. Due interpretazioni del diritto*, Giuffrè, Milano, 1988, pp. 75 ss.

[3] V. Frosini, *Saggi su Kelsen e Capograssi*, cit., pp. 33-34. Para un sugerente desarrollo

Conviene advertir que lo que primariamente ha hecho de Frosini un filósofo del Derecho estimulante y original ha sido su aptitud para superar y trascender, desde el presente, el plano temático de su crítica al idealismo y a la doctrina kelseniana, para situarlo en una órbita de futuro: la de la sociedad tecnológica. La crítica frosiniana al idealismo en nombre de la experiencia, y al kelsenianismo en función de los valores de la humanidad, no han supuesto un regreso a concepciones historicistas o axiológicas del pasado. Su mérito intelectual reside en su capacidad prospectiva para vislumbrar y disenar el horizonte de los derechos y de los valores en la era tecnológica, en la que comenzamos ya a vivir, y que será el contexto inmediato de la experiencia jurídica del porvenir.

De lo expuesto hasta aquí se desprende la pluralidad de aspectos sobre los que se ha proyectado la obra de Frosini y, consiguientemente, desde los que es posible abordarla. De entre ellos, me parece de especial interés y actualidad su concepción de los nuevos derechos de la edad tecnológica. Para centrar este sector del pensamiento filosófico jurídico de Frosini, se puede partir de las dos grandes cuestiones que compendian su consideración doctrinal: ¿qué ha representado la temática de los nuevos derechos de la sociedad tecnológica en la trayectoria científica de Frosini?; y, correlativamente, ¿qué ha representado la obra de Frosini en la conformación teórica de los nuevos derechos?

2. De los derechos naturales del hombre a los derechos del hombre artificial

Los derechos humanos que, durante dos siglos, habían sido tema de estudio y controversia de filósofos del Derecho y de la política, se han convertido tras la Segunda Guerra Mundial en materia de interés general. Hoy resulta fácil comprobar la creciente instalación de la inquietud por los derechos humanos en la consciencia cívica de los hombres y de los pueblos. No obstante los presupuestos y el clima que acompañaron la génesis de la reivindicación de los derechos humanos en el siglo XVIII y el contexto de su situación actual han variado notablemente.

Los teóricos que inspiraron y los políticos que elaboraron las primeras Declaraciones de derechos humanos, los consideraron como reconocimiento de los derechos naturales del hombre. Se trataba de acoger en el Derecho

de la investigación sobre Hans Kelsen, vid. la obra de F. Riccobono, *Interpretazioni kelseniane*, Giuffrè, Milano, 1989.

positivo, en textos normativos de la máxima jerarquía (Constituciones o Declaraciones), los derechos inherentes a todo ser humano, aquellos que le corresponden *per natura*.

Ese universo conceptual y contextual se ha visto profunda y radicalmente modificado por la transformación de los presupuestos antropológicos y cosmológicos que se ha producido en las sociedades tecnológicas del presente. La revolución tecnológica ha redimensionado las relaciones del hombre con los demás hombres, las relaciones entre el hombre y la naturaleza, así como las relaciones del ser humano con su contexto o marco de convivencia. En el curso de estos últimos años pocas cuestiones han suscitado tan amplia y heterogénea inquietud como la que se refiere a las relaciones del hombre con su medio ambiental, en el que se halla inmerso, que condiciona su existencia y por el que, incluso, puede llegar a ser destruido. La plurisecular tensión entre naturaleza y sociedad corre hoy el riesgo de resolverse en términos de abierta contradicción, cuando las nuevas tecnologías conciben el dominio y la explotación sin límites de la naturaleza como la empresa más significativa del desarrollo. Los resultados de tal planteamiento constituyen ahora motivo de preocupación cotidiana. El expolio acelerado de las fuentes de energía, así como la contaminación y degradación del medio ambiente, la utilización de la energía nuclear, o la ingeniería genética, han tenido su puntual repercusión en el habitat humano y en el propio equilibrio psicosomático de los individuos.

No menos importante resulta recordar que nos hallamos en una sociedad donde la informática ha devenido el símbolo emblemático de nuestra cultura, hasta el punto de que para designar el marco de nuestra convivencia se alude reiteradamente a expresiones tales como la «sociedad de la información», o a la «sociedad informatizada». El control electrónico de los documentos de identificación, el proceso informatizado de datos fiscales, el registro y gestión de las adquisiciones comerciales realizadas con tarjetas de crédito, así como de las reservas de viajes, representan algunas muestras bien conocidas de la omnipresente vigilancia informática de nuestra existencia habitual. Nuestra vida individual y social corren, por tanto, el riesgo de hallarse sometidas a lo que Frosini ha calificado, con razón, de «juicio universal permanente»[4]. Ya que, en efecto, cada ciudadano fichado en un banco de datos se halla expuesto a una vigilancia continua e inadvertida, que afecta potencialmente incluso a los aspectos más sensibles de su vida privada; aquellos que en épocas anteriores quedaban fuera de todo control por su variedad y multiplicidad.

[4] V. Frosini, *Cibernética, derecho y sociedad*, cit., p. 178.

2.1. *El horizonte de los nuevos derechos*

En este nuevo contexto se plantean para los derechos humanos dos cuestiones que Frosini juzga prioritarias: ¿hasta qué punto el actual desarrollo científico y tecnológico de la civilización humana permite establecer una relación con la «naturaleza humana», tal como ésta había sido concebida hasta el presente?; y ¿cúales de los viejos «derechos naturales» subsisten en la nueva situación? Porque al haber penetrado en un mundo nuevo, la sociedad tecnológica contemporánea, el hombre debe adaptar los ideales antiguos a la nueva realidad, y el filósofo del Derecho se debe interrogar si el Derecho y los derechos de los que ahora habla son la misma cosa de la que hasta ahora hablaba[5].

Gran parte de los últimos trabajos de Frosini se hallan dirigidos a responder a estas dos cuestiones. En su opinión, la sociedad tecnológica ha producido una nueva imagen mental del hombre, que ha sido definido como «hombre artificial». Dicha definición no se refiere al aspecto material de la existencia humana, sino a su dimensión psicológica: designa un nuevo tipo de hombre que vive en un mundo artificial, en cuanto que ha sido producido por el hombre, no por la naturaleza. El hombre actual se halla sujeto, desde su mismo nacimiento, a una profunda mutación antropológica debida a las mutaciones de sus formas de vida[6]. En nuestro tiempo incluso el atributo que tradicionalmente se consideraba el dato definitorio de la condición humana, es decir, la inteligencia, le ha sido expropiado por las computadoras capaces de desarrollar una «inteligencia artificial». Ella permite a las máquinas memorizar, elaborar y trasmitir información, bien inmaterial indispensable para el desarrollo de la persona y de sus relaciones sociales, en forma artificial. En esas coordenadas se corre el riesgo de que los valores y derechos humanos, en cuanto producto de la conciencia interna o ética interna de la persona, sean suplantados por la absorbente tendencia alienadora de una conciencia externa o heterónoma, expresión de la artificialidad del pensamiento tecnológico.

Vittorio Frosini que posee una clara consciencia tecnológica, en el sentido de un nítido discernimiento de las repercusiones antropológicas y jurídicas del universo artificial producido por la revolución de las nuevas tecnologías, no acepta, sin embargo, una claudicación sin condiciones ante ese fenómeno.

[5] V. Frosini, *L'uomo artificiale. Etica e diritto nell'era planetaria*, Spirali, Milano, 1986, p. 122.

[6] V. Frosini, *Il nuovo diritto del cittadino*, en el vol. col. a cargo de F. Riccobono, *Nuovi diritti dell'età tecnologica*, (Atti del Convegno tenuto a Roma presso la Libera Università Intemazionale degli Studi Sociali, 5/6 maggio 1989), Giuffrè, Milano, 1991, pp. 75 ss.

Su obra representa una estimulante y lúcida advertencia de que los derechos y valores humanos se hallan tradicionalmente adscritos al ámbito de las disciplinas humanísticas. Pertenece, bien que radicados en la era tecnológica, a la naturaleza y a la historia del hombre al ser forma normativa de su existencia. No en vano la experiencia jurídica, la vida ética, la economía, la organización social, la ciencia y la tecnología de la era cibernética, en cada una de las cuales se desenvuelve la conciencia humana conforme a nuevas estructuras del actuar y del conocer, pertenecen a la naturaleza y a la historia del hombre, contribuyendo a ampliar su horizonte. De ahí, que el hombre, al avanzar en la edad nueva, ya dirija su capacidad cognoscitiva y operativa a una materia nueva, ya trate de forma nueva las materias de siempre, sigue siendo él mismo, que vive en un tiempo diverso y que se hace diverso en un mundo que continúa siendo el mundo del hombre[7].

La fidelidad humana a sus propias señas históricas de identidad, amenazadas por la artificialidad, no se traduce en una indiferencia de los derechos respecto al contexto de la sociedad tecnológica. Frosini responde a la segunda cuestión básica sobre el estatuto actual de los derechos, advirtiendo que la era de las nuevas tecnologías ha producido un nuevo ciclo histórico en el devenir de los derechos humanos. La nueva situación se caracteriza lo mismo por la aparición de nuevas libertades, que por un replanteamiento del contenido y función de las antiguas[8]. En este punto la atención intelectual de Frosini que ha analizado de forma atenta nuevas manifestaciones de la libertad (tales como la intimidad, las garantías frente a determinados tratamientos terapéuticos y la ingeniería genética, el derecho a morir dignamente...), así como sobre las repercusiones de determinados fenómenos contemporáneos (como la droga o el terrorismo) sobre el disfrute de las libertades[9], se ha centrado preferentemente en el estudio del nuevo derecho a la liberatad informática.

2.2. *El derecho a la libertad informática*

Frosini concibe libertad informática como el nuevo derecho «de autotutela de la propia identidad informática: o sea, el derecho de controlar (conocer, corregir, quitar o agregar) los datos personales inscritos en las

[7] V. Frosini, *Cibernética, derecho y sociedad*, cit., pp. 151 ss.; id., *Il diritto nella società tecnologica*, Giuffrè, Milano, 1981, pp. 193 ss.; id., *L'uomo artificiale*., cit., pp. 121 ss.

[8] Me he referido a la dimensión generacional de los derechos en mi trabajo *Le generazioni dei diritti umani*, en el vol. col., *Nuovi diritti dell'età tecnologica*, cit., pp. 139 ss.

[9] Cfr. V. Frosini, *L'uomo artificiale*, cit., pp. 89 ss.

tarjetas de un programa electrónico»[10]. En la situación tecnológica propia de la sociedad contemporánea todos los ciudadanos, desde su nacimiento, se hallan expuestos a violaciones de su intimidad perpetradas por determinados abusos de la informática y la telemática. La injerencia del ordenador en las diversas esferas y en el tejido de relaciones que conforman la vida cotidiana se hace cada vez más extendida, más difusa, más implacable.

En el plano jurídico la intimidad se vincula al concepto de libre desarrollo de la personalidad, reconocido como valor fundamental (*Grundwert*) por distintas Constituciones actuales de los Estado de Derecho. Así, por ejemplo, la *Grundgesetz* de la República Federal de Alemania proclama el libre desarrollo de la personalidad (*freie Entfaltung der Personlichkeit*) en su art. 2.1; mientras que la vigente Constitución española de 1978 lo hace en el art. 10.1. Este valor se desglosa, en opinión de Adalbert Podlech, en dos libertades básicas: la libertad general de acción (*allgemeine Handlungsfreiheit*), entendida como libertad para decidir la realización u omisión de determinados actos y la consiguiente facultad para comportarse o actuar de acuerdo con esa decisión; y la **autodeterminación informativa** (*informationelle Selbstbestimmung*), que se refiere a la libertad para determinar quién, qué y con qué ocasión pueden conocer informaciones que conciernen a cada sujeto[11]. El derecho a la autodeterminación informativa (*Recht auf informationelle Selbstbestimmung*), construcción de la doctrina y la jurisprudencia germanas equivalente a la **libertad informática**, tiene una importancia decisiva en las sociedades tecnológicas del presente. Su función se cifra en garantizar a los ciudadanos unas facultades de información, acceso y control de los datos que les conciernen. Pero esa forma de intimidad no se concibe como un valor intrasubjetivo, sino como autodeterminación del sujeto en el seno de sus relaciones con los demás ciudadanos y con el poder público.

El derecho a la libertad informática constituye una modalidad de libertad personal reconocida a los ciudadanos tendente a proteger jurídicamente su «identidad informática». Para el ejercicio del derecho a la libertad informática se precisa reconocer y garantizar las facultades de: conocimiento y acceso por parte de los ciudadanos a las informaciones que les conciernen contenidas en bancos de datos. Por ello, indica Frosini, que al tradicional *habeas corpus* corresponde en las sociedades tecnológicas del presente el *habeas data*[12].

[10] V. Frosini, *Informática y Derecho*, trad. cast., de J. Guerrero y M. Ayerra Redín, Temis, Bogotà, 1988, p. 110.

[11] A. Podlech, *Art. 2 Abs. 1, en Kommentar zum Grundgesetz für die Bundesrepublik Deutschland* (Reihe Alternativkommentare), Luchterhand, Neuwied-Darmstadt, 1984.

[12] V. Frosini, *Il nuovo diritto del cittadino*, cit., p. 77.

El *habeas data* constituye, en suma, un cauce procesal para salvaguardar la libertad de la persona en la esfera informática, que cumple una función paralela, en el seno de los derechos humanos de la tercera generación, a la que en los de la primera generación correspondió al *habeas corpus* respecto a la libertad física o de movimientos de la persona. No es difícil, en efecto, establecer un marcado paralelismo entre la «facultad de acceso» en que se traduce el *habeas data* y la acción exhibitoria del *habeas corpus*.

Se ha repetido hasta la saciedad que las distintas libertades ahondan su raíz histórica en previas situaciones de violación o carencia, a cuyo remedio precisamente se dirigen. De ahí, el nexo inmediato de fundamentación antropológicas de los derechos y libertades en el sistema de necesidades humanas básicas o radicales, por el que algunos venimos abogando. El *habeas corpus* surge como réplica frente a los fenómenos abusivos de privación de la libertad física de la persona, que habían conturbado la Antiguedad y el Medioevo proyectándose, a través del absolutismo, hasta las diversas manifestaciones del totalitarismo de nuestros días. Por ello, la genealogía remota de la institución pudiera cifrarse en el famoso interdicto romano de *homo libero exhibendo* y, en una época posterior, en el recurso medieval aragonés de **manifestación de personas**, que tenía como finalidad prioritaria proteger la libertad personal frente a los desafueros del poder. Dicho recurso entrañaba una facultad del Justicia de Aragón o sus lugartenientes, de las Cortes o Tribunal de Aragón para emitir un mandato a cualquier juez, funcionario o persona que tuviera presa a una persona, pendiente o no de causa, para que se lo entreguen a fin de que no se hiciera violencia alguna contra él, antes de que se dictare sentencia. No obstante este importante precedente la génesis próxima del *Great and efficacious writ of habeas corpus* como lo denominó Blackstone, se debe situar en el paulatino perfeccionamiento consuetudinario del *Common Law* inglés, durante los siglos XIV y XV, que alcanzará su plasmación legislativa en la célebre *Habeas Corpus Act* de 1679. El *habeas corpus* aparece, a partir de esas fuentes, como un recurso procesal por el que se solicita del juez que se dirija al funcionario que tiene una persona detenida y la presente ante él. Se trata, por tanto, de una garantía judicial específica para la tutela de la libertad personal[13].

Al cotejar el habeas corpus y el habeas data se comprueba una inicial coincidencia en lo referente a su naturaleza jurídica. En ambos casos no se trata de derechos fundamentales, stricto sensu, sino de instrumentos o

[13] Cfr. R. Soriano, *El derecho de habeas corpus*, con *Prólogo* de A. E. Pérez Luño, Publicaciones del Congreso de los Diputados, Madrid, 1986.

garantías procesales de defensa de los derechos a la libertad personal, en el caso del *habeas corpus*, y de la libertad informática en lo concerniente al *habeas data*. El *habeas corpus* y el *habeas data* representan, además, dos garantias procesales de aspectos diferentes de la libertad. Así, mientras el primero se circunscribe a la dimensión física y **externa** de la libertad; el segundo tiende a proteger prioritariamente aspectos **internos** de la libertad: la identidad de la persona, su autodeterminación, su intimidad... Si bien, no debe soslayarse que, en las sociedades informatizadas actuales, también la libre actuación pública de los ciudadanos se hallá condicionada por sus posibilidades de acceso a la información.

Pero la diferencia más importante es que el *habeas corpus* aparece como uno de los macanismos procesales básicos para defender la libertad en el marco de lo que en la célebre teoría de los *status*, elaborada por Georg Jellinek serán el *status libertatis* y el *status civitatis*[14]. En tanto que el *habeas data* ha sido fruto del proceso de sucesiva ampliación de los *status*. Ya que su reconocimiento ha sido posible gracias en la medida en que ha calado la exigencia de completar, con nuevos cauces jurídicos que se hicieran cargo de las sucesivas transformaciones operadas en las situaciones subjetivas. Se ha hecho, por tanto, necesario ampliar aquella tipología, pensada para dar cuenta de las libertades y derechos de la primera generación, con el reconocimiento de un *status positivus socialis*, que se haría cargo de los intereses económicos, sociales y culturales propios de la segunda generación[15].

En la actualidad la consagración de la libertad informática y el derecho a la autodeterminación informativa (*Recht auf informationelle Selbstbestimmung*), en el marco de los derechos de la tercera generación, han determinado que se postule el *status* de *habeas data*, concretado, como se ya se ha indicado, en las garantías de acceso y control a las informaciones procesadas en bancos de datos por parte de las personas concernidas.

Es necesario, en definitiva, reconocer la importancia de la informática como nueva forma de poder político y social. No en vano en la sociedad actual la información es poder y ese poder se hace decisivo cuando, en virtud de la informática, convierte informaciones parciales y dispersas en informaciones en masa y organizadas. De ahí, la relevancia actual de la libertad informática como nuevo derecho destinado a garantizar jurídicamente la «identidad informática» de las personas, es decir, su facultad de

[14] G. Jellinek, *System der subjektiven öffentlichen Rechte*, reimp. de la ed. de 1919, Scientia, Aalen, 1964, pp. 81 ss.

[15] Cfr. mi trabajo, *Le generazioni dei diritti umani*, cit., pp. 148 ss.

acceder (*habeas data*) y controlar sus datos personales; así como a restablecer un equilibrio de poderes en el seno de las sociedades tecnológicas[16].

3. Hacia una concepción «heteropoiética» de los derechos humanos

No es tarea fácil sintetizar, en los términos que la brevedad impone a este estudio, lo que ha supuesto para la actual teoría de los derechos humanos el pensamiento de Vittorio Frosini. Como toda obra amplia, profunda y rica en sugerencias e implicaciones, la suya se resiste a ser compendiada en unos rasgos esquemáticos. Si a ello se añade que se trata de una doctrina viva en plena productividad intelectual, que no consiente un balance definitivo, se comprenderá el carácter necesariamente parcial y fragmentario de la valoración que aquí se avanza. Consciente de estos límites arriesgaré la hipótesis de estimar como la aportación más decisiva de Frosini, en el plano que aquí se enjuicia, su contribución a una teoría «heteropoiética» de los derechos humanos.

En la Teoría del Derecho actual han adquirido amplia notoriedad las tesis sustentadas por Niklas Luhmann y por Gunther Teubner en defensa de una visión «autopoiética» del Derecho. Según este planteamiento el Derecho y los derechos humanos serían sistemas basados en la autoreferencia (*Selbsreferenz*) que se constituyen, se conservan, se reproducen y se explican por pautas internas, a través de un proceso de continua autoconstitución. La autopoiesis explica la unidad, la plenitud y clausura del sistema jurídico y del subsistema de los derechos humanos[17].

Debo indicar, de inmediato, mi personal discrepancia de estos enfoques autopoiéticos. Entiendo que lo que tales premisas metódicas pueden tener de bueno, no es nuevo, y que lo que tienen de nuevo no es bueno. El intento más acabado de explicar el Derecho a través de un sistema cerrado, autónomo, autosuficiente en función de un concepto autoreferente de validez normativa se debe a Kelsen; se trata del conocido ideal kelseniano de la pureza metódica: **Reinheit**, como intento de explicar el Derecho sin impor-

[16] Cfr. V. Frosini, *Il nuovo diritto del cittadino*, cit., p. 76 ss.

[17] Sobre la concepción autopoiética del Derecho, cfr. las obras col. a cargo de Gunther Teubner, *Autopoietic Law*, Walter de Gruyter, Berlin, 1988; y *State, Law, Economy as Autopoietic Systems*, Walter de Gruyter, Berlin, 1989, en los que se contienen contribuciones del propio Teubner, así como de Niklas Luhmann, que ha expuesto su teoría de los derechos en su obra *Grundrechte als Institution*, Duncker & Humblot, Berlin, 2ª ed., 1974. Para una crítica de esta concepción vid. mi libro, *Derechos humanos, Estado de Derecho y Constitución*, Tecnos, Madrid, 4ª ed., 1991, pp. 301 ss.

tar modelos externos de la política, la sociología o la ética. Frente a ese ambicioso pero coherente propósito, los actuales empeños de Luhmann y Teubner incurren en la inconsecuencia metodológica de querer fundar la autopoiesis jurídica en base a criterios importados de otras ciencias no jurídicas. Pues, como ellos mismos se ven forzados a reconocer, la idea de sistema autopoiético que les ha servido de modelo procede de la biología, en concreto de las investigaciones biológicas debidas a Varela y Maturana.

Respecto a esos intentos intrasistemáticos, cerrados y autopoiéticos de explicar los derechos humanos, la teoría de Frosini representa una valiosa rehabilitación de los presupuestos extrasistemáticos, de la textura abierta y, en suma, del carácter heteropoiético de tales derechos. Un rasgo peculiar del pensamiento de Frosini ha de encontrarse en el hecho de que ha sido y es un filósofo del Derecho que sin dejar de serlo ha penetrado en el mundo de la ética, de la política, de la literatura, de la sociología y, muy señaladamente, en el de la tecnología contemporánea. Vittorio Frosini ha sido, a la vez, filósofo del Derecho, sociólogo de la cultura y teórico de las nuevas tecnologías. Al actuar así, ha ofrecido una fértil perspectiva de enfoque del Derecho y, en particular, de los derechos humanos abierta a otras regiones actuales de la ciencia y la tecnología. Gracias a Frosini un importante acervo de categorías y conceptos de la cultura científica y tecnológica contemporánea se han incorporado al *modus operandi* de la Filosofía del Derecho y al análisis de los derechos humanos. Baste pensar en su contribución, decidida y decisiva, en la tarea de acuñar, elaborar y difundir el concepto de libertad informática.

Los derechos humanos surgieron en la modernidad como respuestas jurídicas a las exigencias éticas y los problemas políticos de aquella coyuntura histórica. Hoy ese contexto ha variado profundamente, fruto de la revolución tecnológica. Por eso una teoría de los derechos encerrada autopoiéticamente en sí misma no sólo es incapaz de explicar, de forma satisfactoria, la función de los derechos en la experiencia política, científica y cultural del presente; es incluso inútil (o, en el peor de los casos, deformadora) de su concepto. El mérito de Frosini estriba en haber sido uno de los primeros teóricos de los derechos humanos atentos a los apremios de la sociedad tecnológica. Pocos antes que él se habían tomado en serio la faena de construir una teoría de los derechos «heteropoiéticamente» abierta, y responsablemente comprometida con la respuesta a las nuevas necesidades y exigencias de los hombres que viven en la era de la informática.

Vittorio Frosini reclama de los juristas, los filósofos del Derecho y los teóricos de los derechos humanos de nuestro tiempo una «coscienza tec-

nologica»[18]; es decir, una actitud reflexiva crítica y responsable ante los nuevos problemas que, en las diversas esferas del acontecer social suscita la tecnología, y ante los que ni el Derecho ni los derechos humanos pueden pemmanecer insensibles. La exigencia de Frosini complica sobremanera la labor de los teóricos de los derechos, porque les obliga a ampliar el angosto horizonte de las autoreferencias normativas, con la apertura hacia los estímulos de la ciencia y la tecnología. Pero sólo mostrando sensiblidad a esa exigencia la teoría de los derechos humanos será capaz de responder a los retos de la sociedad tecnológica actual; lo que es tanto como decir que sólo en virtud de esa «coscienza tecnologica» la teoría de los derechos tendrá sentido.

La influencia de Vittorio Frosini en la doctrina actual de los derechos humanos ha sido dilatada y provechosa. Su repercusión no ha quedado limitada a sus colaborades y discípulos, en sentido estricto; porque cuantos hoy nos planteamos el estudio de los derechos humanos desde la consciencia de la era tecnológica somos esencialmente deudores de sus ensenanzas.

[18] V. Frosini, *Il diritto nella società tecnologica*, cit., p. 270; id., *L'uomo artificiale*, cit., p. 141.