RIVISTA ITALIANA DI INFORMATICA E DIRITTO

Periodico internazionale di diritto, giustizia e tecnologie

2•2025

SEZIONI MONOGRAFICHE

***Le due facce della rivoluzione digitale, tra emergenze e tecnologie* dual-use**
a cura di Paolo Passaglia

❐

Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement - Parte 1
a cura di
Gaetana Morgante e Gaia Fiorinelli

❐

I dati in ambito pubblico tra esercizio della funzione amministrativa e regolazione del mercato
a cura di
Marco Bombardelli, Simone Franca, Anna Simonati

diretta da **Sebastiano Faro • Marina Pietrangelo**

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

anno VII • periodicità semestrale • ISSN 2704-7318

www.rivistaitalianadiinformaticaediritto.it

Consiglio Nazionale delle Ricerche

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

Organi

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.

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 Mariasole Rinaldi
Redazione 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

2·2025

Indice

Sezioni monografiche

Le due facce della rivoluzione digitale, tra emergenze e tecnologie *dual-use*

a cura di Paolo Passaglia

Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement

a cura di Gaetana Morgante e Gaia Fiorinelli

Indagini criminologiche, diritto penale, diritto internazionale

I dati in ambito pubblico tra esercizio della funzione amministrativa e regolazione del mercato

a cura di Marco Bombardelli, Simone Franca, Anna Simonati

Sezione monografica

Le due facce della rivoluzione digitale, tra emergenze e tecnologie dual-use

a cura di

Paolo Passaglia

RIVISTA ITALIANA
DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0233 • articolo sottoposto a peer review • pubblicato in anteprima il 1 ago. 2025

Paolo Passaglia

Nuove tecnologie ed emergenza di nuove forme di esclusione sociale

Le nuove tecnologie offrono ai consociati grandi opportunità nell'esercizio dei diritti. Al contempo, però, per coloro che ad esse non hanno accesso sono fattori di nuove o maggiori esclusioni sociali. Per far fronte a queste conseguenze negative, il diritto si è concentrato, per anni, soprattutto sulla lotta contro i divari digitali; l'impossibilità di eliminare in radice questi divari richiede tuttavia di adottare una prospettiva di analisi che faccia i conti con questa realtà. L'articolo parte da queste considerazioni per valutare gli effetti che possono derivare dal riconoscimento di due diritti. Il primo è il diritto di accesso alle nuove tecnologie, che è ormai ampiamente consolidato e per il quale la configurazione alla stregua di un diritto sociale è senz'altro prevalente. Il secondo diritto, che è venuto emergendo in dottrina soprattutto negli anni più recenti (anche in relazione all'esperienza pandemica), è il diritto a non utilizzare le nuove tecnologie, un diritto che può avere due concretizzazioni principali: per un verso, quella del diritto a rifiutare di ricorrere alle nuove tecnologie, per l'altro quella di consentire a chi non è in grado di utilizzare le nuove tecnologie di non essere escluso dall'esercizio di diritti, rendendo imprescindibile l'esistenza di alternative. In quest'ultima accezione, il diritto a non utilizzare le nuove tecnologie rappresenta una protezione di grande rilievo contro nuove possibili esclusioni sociali.

Nuove tecnologie – Esclusione sociale – Digital divide – Diritto di accesso alle nuove tecnologie
Diritto a non utilizzare le nuove tecnologie

New technologies and the emergence of new forms of social exclusion

New technologies provide great opportunities for individuals to exercise their rights. At the same time, however, technologies cause new or increased social exclusions for those who do not have access to them. To cope with these negative consequences, the law has focused, for years, primarily on struggling against digital divides; the impossibility of eradicating these gaps, however, requires adopting an approach that takes into account this reality. Based on these considerations, the paper aims to assess the effects that may result from recognizing two rights. The first is the right to access new technologies, which is now widely established and mostly defined as a social right. The second right, which has been emerging in doctrine, especially in more recent years (also concerning the experience during the Covid pandemic), is the right not to use new technologies, a right that can have two main implementations: on the one hand, that of the right to refuse to use new technologies, and on the other hand, that of allowing those who are unable to use new technologies not to be excluded from the exercise of rights, making it essential the existence of alternative means. In the latter sense, the right not to use new technologies represents a very important protection against possible new social exclusions.

New technologies – Social exclusion – Digital divide – Right to access new technologies
Right not to use new technologies

L'Autore è professore ordinario di Diritto comparato, Università di Pisa

Questo contributo fa parte della sezione monografica *Le due facce della rivoluzione digitale, tra emergenze e tecnologie* dual-use, a cura di Paolo Passaglia

1. Introduzione

Nell'approcciarsi alle nuove tecnologie, il giurista oscilla, da sempre, tra due atteggiamenti significativamente divergenti. Da un lato, la novità viene associata all'ignoto e, da lì, al pericolo: l'incedere del progresso tecnologico è costantemente visto come una fonte potenziale di nuove insidie. In tal senso, può farsi efficacemente riferimento all'attenzione che, sin dagli anni Novanta (se non prima), ha attirato la tematica della protezione dei dati personali, con preoccupazioni che si rinnovano periodicamente, in concomitanza con il manifestarsi di nuovi strumenti (si pensi, negli ultimi tempi, all'irrompere dei software di intelligenza artificiale). Dall'altro lato, però, è pressoché unanime il riconoscimento delle potenzialità che il progresso tecnologico offre in termini di esercizio di diritti individuali: le nuove tecnologie, infatti, consentono di fare cose che prima erano impensabili ovvero di farle in tempi e/o in modi incommensurabilmente più efficaci che in passato. Dallo sviluppo delle forme di comunicazione all'emersione di forme di democrazia partecipativa, passando per l'accesso all'informazione e per molte altre vicende che connotano la vita degli esseri umani, gli esempi che esprimono le potenzialità dischiuse dal progresso tecnologico degli ultimi anni sono troppo evidenti perché se ne debba qui dare conto.

La duplicità degli atteggiamenti non si è peraltro tradotta in una bipolarizzazione, ma piuttosto in una compenetrazione, certo agevolata anche dall'emergenza, sotto la voce "pericoli", di un ulteriore fattore atto a mitigare eventuali entusiasmi: nel momento in cui si riconoscono i benefici delle nuove tecnologie, non ci si può infatti esimere dall'inserire, nel novero dei rischi, un'ulteriore voce – di peso – che si collega all'eventualità che i benefici recensiti non siano aperti all'insieme dei consociati, con la conseguenza di creare o di aggravare forme di diseguaglianza, se non addirittura di esclusione sociale.

Proprio su questo aspetto si ritiene utile, in questa sede, soffermarsi, onde porre in risalto il carattere bifronte che, da un punto di vista giuridico (o, se vogliamo, costituzionalistico), le nuove tecnologie possono rivelare.

La ragione di questa scelta non è riconducibile al manifestarsi di situazioni nuove o di riforme normative recentemente intervenute. La novità che può addursi consiste, piuttosto, nell'emergere (*recte*, nel consolidarsi) di nuovi punti di vista dai quali osservare i fenomeni.

In effetti, la ricerca di un equilibrio tra i benefici delle nuove potenzialità e i pericoli delle nuove esclusioni è stata declinata, per lungo tempo, nell'ottica di creare le condizioni per superare o eludere i secondi (anche) al fine di generalizzare i primi. Più di recente, l'approccio alla tematica è divenuto più complesso, sia perché i benefici si pongono sempre meno alla stregua di presupposti assiomatici sia, soprattutto (?), perché la loro generalizzazione è risultata assai più ardua di quanto potesse postularsi.

Per chiarire il senso di quanto precede conviene adottare una chiave di lettura basata sull'esistenza di due diritti, collegati ma distinti, attraverso i quali esaminare i rapporti tra i suddetti "benefici" e "pericoli": in sostanza, se si è soliti ragionare in merito a un diritto di utilizzare le nuove tecnologie, non può trascurarsi l'ipotesi di un diritto a *non* utilizzarle.

Le due tipologie di situazioni soggettive, che non hanno avuto una storia parallela, giacché una

è emersa ben prima dell'altra, richiedono un qualche chiarimento preliminare.

Il diritto di utilizzare le nuove tecnologie può prestarsi a fraintendimenti, specie in considerazione dell'esistenza di un "diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni e con i gestori di pubblici servizi statali", riconosciuto dall'art. 3, rubricato "Diritto all'uso delle tecnologie", del Codice dell'amministrazione digitale (d.lgs. 7 marzo 2005, n. 82). In realtà, per diritto di utilizzare le nuove tecnologie si vuole intendere, in questa sede, un diritto generale ad accedervi (e quindi a utilizzarle). Così posto, il diritto di cui si discorre può essere validamente configurato alla stregua della risultante di un diritto presupposto, che è quello di accesso a Internet: per fruire, infatti, delle possibilità offerte dalle nuove tecnologie, il poter disporre di una connessione è pressoché indispensabile, vuoi perché molte tecnologie sono attive esclusivamente in rete, vuoi perché è solo grazie alla rete che la stragrande maggioranza delle tecnologie fruibili anche offline dispiegano tutte le loro potenzialità. Sulla scorta di questa premessa, il diritto di accesso (a Internet e quindi) alle nuove tecnologie può essere identificato come uno dei temi che per primi sono stati capaci di attirare l'interesse dei giuristi – e in particolare dei costituzionalisti – per le implicazioni della rivoluzione digitale, al punto che la tematica poteva dirsi già al centro del dibattito scientifico nell'ultimo scorcio del primo decennio del secolo[1], in parallelo, peraltro, con alcune significative prese di posizione giurisprudenziali[2].

Ben più recente è l'emersione di un autonomo diritto a *non* utilizzare le nuove tecnologie, che velleità di simmetria potrebbero far riassumere sotto l'etichetta – invero non del tutto perspicua – del diritto a non accedere alle tecnologie e quindi a Internet. Il suo riconoscimento può dirsi, almeno per certi versi, ancora in fase di gestazione, dopo che se ne sono avvertite le potenziali ricadute concrete, soprattutto nel periodo della pandemia[3].

Nonostante, come si cercherà di dimostrare, i due diritti abbiano collegamenti tutt'altro che accidentali, per chiarezza espositiva conviene trattarli separatamente, per poter restituire – si auspica – una prospettiva di un qualche interesse in merito, appunto, al rapporto tra le nuove tecnologie e l'emergenza di nuove forme di esclusione sociale.

2. Il diritto ad accedere alle nuove tecnologie

L'emersione di un diritto ad accedere alle nuove tecnologie, dall'angolo visuale ampio dell'accesso a Internet, si è strettamente collegata alla constatazione che le "magnifiche sorti e progressive" di un mondo tecnologizzato non si dischiudevano necessariamente di fronte all'insieme dei consociati. L'accrescimento del coefficiente di sviluppo informatico che penetrava rapidamente nella società ha anzi reso ben presto chiaro che nuove forme di

1. Nella dottrina italiana, la tematica dell'accesso a Internet si è sviluppata soprattutto in parallelo con alcune proposte di inserimento dell'affermazione di questo diritto all'interno della Costituzione. Al riguardo, può ricordarsi, tra le primissime iniziative, un incontro di studio i cui atti sono poi confluiti in un fortunato volume Pietrangelo 2011.
2. Il riferimento va, in particolare, alla decisione del *Conseil constitutionnel* francese sulla *Loi Hadopi I*, in cui si è teorizzato un vero e proprio diritto di accesso a Internet, come componente della libertà di espressione (dec. n. 2009-580 DC, del 10 giugno 2009, oggetto di studio anche da parte della dottrina italiana: cfr. Votano 2009; Carotti 2010; Lucchi 2010; Lucchi 2011, nonché, volendo, Passaglia 2009). Anche in precedenza, peraltro, erano state rese decisioni che, pur senza proporre definizioni, quanto meno postulavano – in maniera inequivocabile – un tale diritto di accesso: a tale proposito, può ricordarsi anche una pronuncia resa dalla Corte costituzionale italiana, la cui fortuna, nel dialogo giurisprudenziale transnazionale, è stata forse pregiudicata dalla sua stringatezza (cfr. la sentenza 21 ottobre 2004, n. 307, commentate da Pace 2004, e, successivamente, da Pizzetti 2008).
3. È appena il caso di rilevare che il diritto a non utilizzare le nuove tecnologie è tutt'altra cosa rispetto al c.d. diritto alla disconnessione, come si è affermato, dapprima, in Francia e, poi, in vari altri Stati, Italia compresa: tale diritto non si riferisce, infatti, all'utilizzo delle tecnologie in quanto tali, ma ha di mira, piuttosto, una protezione del lavoratore e la rigorosa delimitazione dell'orario di lavoro. Per l'inquadramento della tematica, in riferimento all'ordinamento italiano, v. Altimari 2021; in una prospettiva europea, v. Zoppoli 2023.

diseguaglianza erano destinate a manifestarsi, fino a creare vere e proprie divisioni, per non dire fratture. In questa logica ha assunto un'importanza crescente il concetto di *digital divide*, il quale, specie in alcune sue traduzioni, appare quanto mai indicativo della gravità delle conseguenze potenziali delle nuove tecnologie: se, infatti, in italiano il "*divide*" viene tradotto con il termine "divario", in francese, ad esempio, si propone una assai più ruvida "*fracture*".

Ponendosi su questa lunghezza d'onda, la situazione soggettiva recante la pretesa o l'aspettativa di accedere alle nuove tecnologie è stata – quasi inevitabilmente – analizzata alla luce dei possibili impedimenti che potessero frustrarla. E allora si è presa coscienza della pluralità di divari che percorrono le società, e che impongono di ragionare dell'accesso a Internet (e alle nuove tecnologie) in chiave definitoria, con ciò intendendo, non semplicemente la prospettiva del riconoscimento (ormai abbastanza scontato) dell'esistenza di un *diritto*, ma anche – e soprattutto – il chiarimento in ordine al *tipo* di diritto eventualmente da riconoscere.

2.1. I divari digitali

Pur senza alcuna pretesa di completezza, e a fini puramente evocativi, possono essere individuati almeno cinque basi di divaricazione all'interno della società che ostacolano, fino a impedirla, la diffusione generalizzata dall'accesso alle nuove tecnologie.

2.1.1. Il divario geografico

Internet e le tecnologie che a esso si collegano non hanno una diffusione uniforme sull'insieme del territorio. È inevitabile che le condizioni di fruizione mutino in maniera significativa a seconda che ci si trovi in centri abitati di grandi dimensioni ovvero di dimensioni molto modeste, per tacere delle campagne o di altre aree a densità di popolazione bassissima e/o di problematica raggiungibilità. Le divergenze nella fruibilità divengono assolute in quelle zone che non sono raggiunte dalla rete[4]. Se è vero che, in talune aree del mondo, questa eventualità è tendenzialmente molto rara, le profonde discrasie rispetto ad altre regioni, in un quadro, come quello di Internet, che è necessariamente transnazionale, evocano problematiche che sono, a un tempo, giuridiche e geopolitiche.

2.1.2. Il divario economico

Un discorso molto simile, *mutatis mutandis*, a quello condotto su base geografica può essere proposto relativamente al divario fondato su motivazioni economiche, le quali possono riverberarsi sulla disponibilità di hardware, di software e/o di accesso alla Rete.

Proprio per ovviare all'esistenza di divari di matrice economica e geografica, è venuta in rilievo la nozione di "servizio universale", attualmente delineata, per l'Italia, dall'art. 94, comma 1, del d.lgs. 1° agosto 2003, n. 259 (Codice delle comunicazioni elettroniche): "Su tutto il territorio nazionale i consumatori hanno diritto ad accedere a un prezzo accessibile, tenuto conto delle specifiche circostanze nazionali, a un adeguato servizio di accesso a internet a banda larga e a servizi di comunicazione vocale, che siano disponibili, al livello qualitativo specificato, ivi inclusa la connessione sottostante, in postazione fissa, da parte di almeno un operatore". Il riferimento alla nozione di "consumatore" tradisce una impostazione che, dal punto di vista costituzionalistico, suona senz'altro riduttiva, non fosse altro perché rischia di non porre adeguatamente in risalto la dimensione di lotta contro le diseguaglianze che pervadono la società, almeno quando queste si rivelano inaccettabili[5]. Al netto di questa riserva, ciò che rileva è, comunque, l'idea che l'accesso a Internet, con quanto ne consegue (quindi anche in termini di accesso alle nuove tecnologie), non possa essere lasciato integralmente al libero dispiegarsi del

4. Non si tratta, peraltro, della semplice collocazione geografica, che è anzi solo – tutt'al più – un presupposto: la maggiore o minore fruibilità della rete dipende, infatti, per l'essenziale dalle infrastrutture che consentono l'accesso e che ne disegnano l'efficacia. In questa logica, il divario che si è qui definito "geografico" ben può essere definito anche come "infrastrutturale".
5. Sull'accentuazione della dimensione della lotta alla povertà nella ridefinizione del concetto di servizio universale, prima maggiormente ancorato alla dimensione geografica, v. da Empoli 2021.

mercato, imponendosi un intervento pubblico rivolto alla protezione dei soggetti più deboli[6].

2.1.3. Il divario fisiologico

Un divario digitale inevitabile percorre la società anche in riferimento alla disabilità. La tematica è stata posta al centro dell'attenzione sin dai primi anni della rivoluzione digitale[7], e ha prodotto, ad esempio, un impianto normativo teso a incrementare quanto più possibile l'accessibilità e l'usabilità dei siti Internet[8]. Il tema specifico, ovviamente, rappresenta la faccia tecnologica del complesso prisma dell'applicazione effettiva del principio di eguaglianza alle persone con disabilità[9].

2.1.4. Il divario culturale

Uno degli ostacoli più delicati da superare per la fruizione della Rete riguarda le competenze informatiche dei potenziali utenti, in ragione delle quali una parte della popolazione è radicalmente esclusa dall'accesso alle nuove tecnologie, mentre altri segmenti hanno un accesso (più o meno) fortemente condizionato dai limiti discendenti da competenze non del tutto adeguate. Questo divario, che può genericamente definirsi come "culturale", è quello che si collega direttamente alla tematica della "alfabetizzazione digitale".

Quest'ultima espressione è senz'altro evocativa e ottimistica, ma rischia di rivelarsi pericolosamente fuorviante. La carica ottimistica risiede nel parallelo implicito che si propone con l'opera di alfabetizzazione che, in Italia come in molti altri paesi, ha condotto a rendere il fenomeno dell'analfabetismo assolutamente marginale.

Ora, di questo processo, l'asse portante – anche se non certo l'unico, trattandosi anzi di una dinamica assai complessa[10] – è da individuare nell'istituzione scolastica[11], il che può indurre a riproporre per l'alfabetizzazione digitale lo stesso schema operativo. Chiaramente, che si apprendano a scuola competenze informatiche è non solo opportuno, ma assolutamente necessario, ciò che del resto è oggetto di attenzione, con alterne fortune, da parte dei pubblici poteri[12]. Il punto, però, è che l'esclusione sociale non colpisce tanto la popolazione in età scolare, quanto piuttosto le fasce anagraficamente più avanzate[13], il che rende indispensabili azioni che vadano ben oltre le istituzioni scolastiche. In tal senso, è significativo, ad esempio, che, nel Piano nazionale di ripresa e resilienza, si preveda l'istituzione di un "Servizio Civile Digitale", consistente in "una rete di *giovani volontari* provenienti da contesti diversi di tutta Italia che aiuteranno gli utenti a rischio di esclusione digitale con servizi di facilitazione ed educazione affinché acquisiscano e migliorino le competenze digitali"[14].

Il punto più delicato, nel quale il parallelismo suggerito tra la lotta storica all'analfabetismo e l'alfabetizzazione digitale contemporanea presenta la massima criticità, risiede però nel fatto che, una volta appreso a leggere e a scrivere, queste competenze tendenzialmente si conservano, salvi i casi di analfabetismo di ritorno, che non debbono né possono essere sottovalutati, ma che

6. Il collegamento tra l'affermazione di un diritto universale e la qualificazione dell'accesso a Internet come "un diritto sociale, o meglio una pretesa soggettiva a prestazioni pubbliche" è messo in rilievo, tra i primissimi, da Frosini 2011 (p. 7).
7. Cfr., in part., Ridolfi 2002.
8. Il riferimento obbligato è, qui, alla legge 9 gennaio 2004, n. 4, recante "Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici" (c.d. Legge Stanca).
9. Al riguardo, v., in generale e in tempi relativamente recenti, Arconzo 2020. La disciplina e le azioni positive poste in essere, a livello anche europeo, per la concretizzazione della fruizione della rete da parte delle persone con disabilità sono analizzate da Sica 2022.
10. Cfr. De Mauro 1963/2011 (spec. p. 51 ss.).
11. V., *ex multis*, De Fort 1995.
12. Sul tema, v. da Empoli 2023.
13. "Con una popolazione di età media più elevata rispetto al resto d'Europa, una delle sfide più ardue per l'Italia è certamente il coinvolgimento di individui appartenenti a fasce d'età più avanzate": così da Empoli 2023 (p. 4).
14. Intervento 1.7 (Competenze digitali di base – Competenze di base nella lotta all'emarginazione digitale; enfasi testuale). Sul punto, v. Cocchiara 2023 (spec. p. 206 ss.).

comunque si traducono in una regressione molto significativa solo in percentuali tutto sommato molto contenute: con questa riserva, l'alfabetizzazione può essere considerata una acquisizione che, tendenzialmente, si consolida o si conferma. L'alfabetizzazione digitale, di contro, è strutturalmente provvisoria, giacché le competenze che si acquisiscono oggi diverranno obsolete domani, quando muteranno hardware e software, nonché, magari, le forme di comunicazione e di utilizzo degli strumenti: la logica non può quindi essere quella di una formazione *una tantum*, ma quella di una formazione continua, che è estremamente difficile per i pubblici poteri garantire su vasta scala e che di conseguenza richiede, in primo luogo, un'autodeterminazione individuale. Tenendo conto di questa esigenza, più che all'uso di strumenti, la formazione iniziale (quella scolastica) dovrebbe semmai mirare all'acquisizione di una capacità di analisi critica degli strumenti informatici, e quindi anche della loro evoluzione. Su questo crinale, però, il discorso si allontana troppo dal terreno su cui un giurista può muoversi senza improvvisare troppo. Del resto, l'aver constatato la distanza tra ciò che le istituzioni scolastiche possono assicurare e le esigenze di aggiornamento pressoché permanente è già più che sufficiente a dar conto della difficoltà di adattare alla lotta al divario digitale culturale categorie pensate per altro.

2.1.5. Il divario imposto

La quinta tipologia di divari digitali è affatto particolare, giacché muove dall'implicito riconoscimento dell'*assenza* di un divario, che infatti viene prodotto dai pubblici poteri. È quanto si verifica allorché questi ultimi pongono un divieto, totale o parziale, di accesso alla Rete o a certe tecnologie: i pubblici poteri, anziché impegnarsi contro potenziali cause di esclusione sociale, si pongono, nella specie, all'origine delle stesse.

Questo tipo di divari si riscontra con una frequenza non trascurabile nei sistemi autoritari, là dove, tra le altre cose, al blocco di Internet si fa ricorso per rendere più difficoltosa la diffusione di critiche e/o di manifestazioni contrarie ai titolari del potere[15]. I sistemi democratici, tuttavia, non sono immuni da applicazioni, sebbene su scala diversa. Un esempio emblematico attiene al divieto di accesso a Internet che vari ordinamenti europei, tra cui quello italiano, prevedono per i detenuti o almeno per una parte di essi[16]. L'enucleazione di divari imposti potrebbe arricchirsi di tutti quei casi nei quali si pongano divieti di accesso legati a particolari condizioni ovvero conseguenti al compimento di determinati atti[17]. La variabilità delle situazioni renderebbe assai ardua la redazione di un elenco di fattispecie, che avrebbe peraltro, almeno qui, un interesse piuttosto limitato, dal momento che i divari digitali imposti pongono problemi significativamente diversi rispetto agli altri divari, sotto molti punti di vista, ma in particolare – lo si è già rilevato – per quanto concerne il collegamento con le esclusioni sociali. Avuto riguardo ai fini della presente trattazione, non pare dunque il caso di soffermarvisi ulteriormente.

2.2. Le definizioni dell'accesso

L'insieme dei divari digitali che si sono passati in rassegna (con l'eccezione dell'ultimo) impongono all'ordinamento giuridico di strutturare forme di risposta alle esigenze sociali volte ad assicurare l'accesso alle nuove tecnologie a chi ne sia escluso.

La soluzione più immediata è, ovviamente, quella di riconoscere all'accesso lo *status* di un *diritto*, ciò che è ormai quasi unanimemente accolto. L'eccezione forse più significativa consiste nella posizione di chi contesta l'esistenza di un diritto all'accesso come diritto a sé stante: la sua protezione, infatti, sarebbe il portato della sua strumentalità rispetto ai diritti che grazie alla tecnologia possono essere esercitati. Così, l'accesso alle nuove tecnologie si declinerebbe, di volta in volta, come strumento della libertà di espressione, del diritto al lavoro, del diritto alla salute, e così via, a seconda

15. Gli esempi sono davvero troppi per essere anche semplicemente menzionati. Per un quadro di marca comparatistica, v., anche per ulteriori riferimenti, Formici 2023.
16. In proposito, v. Camillieri 2024.
17. Al riguardo, può ricordarsi che la precitata legge *Hadopi I* è stata censurata dal *Conseil constitutionnel* (v. *supra*, nota 2) proprio nella parte in cui limitava l'accesso a Internet (mediante l'interruzione della fornitura del servizio a domicilio) per i detentori di credenziali di connessione utilizzando le quali si fossero commesse violazioni del diritto d'autore.

di ciò che attraverso la tecnologia l'utente andrebbe concretamente a fare[18].

L'impostazione è senz'altro interessante, sul piano teorico. A ben vedere, però, la questione rischia di ridursi in larga misura a una controversia terminologica: che l'accesso alle nuove tecnologie sia qualificato come "diritto" oppure no può in effetti cambiare molto poco, se resta fermo il fatto che, in ogni caso, l'accesso ha la funzione di far esercitare altri diritti o di farli esercitare in forme diverse da quelle tradizionali. Altrimenti detto, la strumentalità è una caratteristica ineliminabile dell'accesso di cui si discorre, sia che questo venga definito alla stregua di un "diritto" (appunto, strumentale) sia che si preferisca ricondurlo a un (semplice) mezzo attraverso il quale un certo diritto o certi diritti vengono esercitati.

A rilevare è, in buona sostanza, come questo "strumento" venga concretamente protetto all'interno dell'ordinamento. E, ponendosi in quest'ottica, probabilmente il riferimento al "diritto" può essere utile per trovare definizioni più immediate. Si prospetta, infatti, un'alternativa piuttosto netta a seconda che si concepisca l'accesso alle nuove tecnologie come una libertà oppure come una pretesa di prestazione.

Il rivendicare una *libertà*, per l'essenziale, si traduce nella mera aspettativa che i pubblici poteri non interferiscano con il suo godimento: ci si deve quindi porre semplicemente il problema di fare in modo che non si interrompa con atto dell'autorità la fruizione dell'accesso alla tecnologia. Una tale impostazione è emersa in riferimento all'accesso a Internet nelle prime decisioni che su di esso si sono pronunciate e che, indirettamente o *expressis verbis*, lo hanno ricollegato alla libertà che per prima e più di ogni altra sulla Rete si esercita: la libertà di espressione[19]. Poiché l'obiettivo qui perseguito è quello di indagare il rapporto tra nuove tecnologie ed esclusione sociale, è chiaro che questa impostazione non possa presentare un grande interesse: se, infatti, si rivendica una libertà, ciò significa che potenzialmente si è in grado di esercitarla, e la si rivendica perché se ne è esclusi fintantoché i pubblici poteri non si astengano dall'interferenza sulla libertà individuale. Tra i divari digitali che si sono elencati, è soprattutto il quinto che viene qui in rilievo. Ma il quinto è proprio quello che, come

18. "[T]echnology is an enabler of rights, not a right itself": così Cerf 2012. Una posizione almeno in apparenza non dissimile è stata adottata dalla Corte suprema indiana, quando i membri del collegio, nel decidere il caso *Anuradha Bhasin v. Union of India*, W.P.(C) No.-001031/2019 (10 gennaio 2020), hanno precisato di limitarsi a "declaring that the right to freedom of speech and expression under Article 19(1)(a), and the right to carry on any trade or business under 19(1)(g), using the *medium* of internet is constitutionally protected" (§ 28, enfasi aggiunta).

19. La libertà di espressione è al centro, in particolare, della prima grande decisione concernente Internet, quella resa dalla Corte suprema statunitense nel caso *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997), in cui si è ricostruito l'accesso a Internet come la condizione per l'individuo di beneficiare di "a wide variety of communication and information retrieval methods" (p. 851). A distanza di venti anni, la stessa Corte è tornata sul tema (in occasione del caso *Packingham v. North Carolina*, 582 U.S. 98, del 2017), riproponendo il collegamento tra la libertà di accedere alla Rete e i suoi effetti in termini di esercizio della libertà di espressione: "A fundamental principle of the First Amendment is that all persons have access to places where they can speak and listen, and then, after refection, speak and listen once more. […] While in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is cyberspace […], and social media in particular" (p. 104). Nell'intervallo temporale tra le due decisioni, tuttavia, altrove il collegamento tra (libertà di) accesso a Internet e libertà di espressione era stato ancora più chiaramente delineato: il riferimento va alla precitata decisione del *Conseil constitutionnel* n. 2009-580 DC (v. *supra*, nota 2), secondo cui, se "aux termes de l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789: 'La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme' tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi", "en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services" (considérant 12).

si diceva, nell'economia del presente scritto è di minore interesse.

Se, invece, si tratta della pretesa di una prestazione, non ci si accontenta, evidentemente, della mancata interferenza, ma si prefigura un obbligo positivo in capo alle pubbliche autorità (o ai privati incaricati di fornire un pubblico servizio), che debbono impegnarsi affinché l'accessibilità alle nuove tecnologie, attraverso Internet, sia assicurata, all'uopo rimuovendo gli ostacoli di vario tipo che possono impedirlo. Nella logica di questo tipo di richieste, l'accesso a Internet assume una valenza che richiama strettamente quella dei diritti sociali[20], il che si coniuga in maniera inequivocabile con la problematica delle possibili esclusioni sociali, le quali implicano azioni dei pubblici poteri volte a evitarle o a limitarne gli effetti. In questa prospettiva, appare piuttosto lineare il giungere a configurare la mancata possibilità di accesso alle nuove tecnologie, per uno dei primi quattro divari elencati in precedenza, come il risultato di uno de "gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana", ostacoli che, ai termini dell'art. 3, secondo comma, della Costituzione repubblicana, "[è] compito della Repubblica rimuovere"[21].

Questi approdi argomentativi appaiono, ormai, almeno nel contesto italiano, sufficientemente solidi da non richiedere speciali dimostrazioni. Del resto, l'impegno dei pubblici poteri per il potenziamento della fruizione e per il miglioramento della fruibilità di Internet è troppo consolidato – almeno nelle dichiarazioni di principio – per potersi avanzare dubbi in merito all'inserimento dell'accesso alle nuove tecnologie nel quadro delle politiche che connotano il *Welfare State*[22].

Superando, però, il piano teorico e scendendo più nel concreto, qualche considerazione può forse essere aggiunta. Se la tutela del diritto di accesso alle nuove tecnologie implica necessariamente, per quanto si è venuti dicendo, un impegno in termini economici da parte dei pubblici poteri, è chiaro che si imporrà un bilanciamento tra diversi diritti che richiedono prestazioni, nella cornice di una limitatezza insuperabile – ai termini dell'art. 81 della Costituzione – delle risorse disponibili. Gli stanziamenti a favore dell'accesso alle nuove tecnologie saranno quindi l'espressione di un giudizio di prevalenza che il decisore politico avrà ad esso riconosciuto rispetto ad altri diritti concorrenti. Come dire che, affinché siano giustificate le spese che si sostengono per potenziare e diffondere l'accesso alle nuove tecnologie, è necessario che possano

20. Un approccio fortemente ispirato alla definizione dell'accesso alle nuove tecnologie come diritto sociale emerge, in particolare, nella sentenza n. 307 del 2004 della Corte costituzionale (sulla quale, v. *supra*, nota 2), in cui, in effetti, si controverteva di riparto di competenze tra Stato e Regioni con riferimento ad allocazioni finanziarie a beneficio di determinati soggetti finalizzate all'acquisto di hardware idoneo alla connessione a Internet. Particolarmente nitida nell'affermare l'esistenza di un obbligo di *facere* dei pubblici poteri in vista del soddisfacimento di un diritto dei singoli consociati è stata la *Sala Constitucional de la Corte Suprema de Justicia* della Costa Rica, nella *sentencia* 30 luglio 2010, n. 12790: "En este momento, el acceso a estas tecnologías se convierte en un instrumento básico para facilitar el ejercicio de derechos fundamentales como la participación democrática (democracia electrónica) y el control ciudadano, la educación, la libertad de expresión y pensamiento, el acceso a la información y los servicios públicos en línea, el derecho a relacionarse con los poderes públicos por medios electrónicos y la transparencia administrativa, entre otros. […] En este contexto de la sociedad de la información o del conocimiento, se impone a los poderes públicos, en beneficio de los administrados, promover y garantizar, en forma universal, el acceso a estas nuevas tecnologías" (Considerando V).

21. Sul fondamento della tutela costituzionale di Internet e dell'accesso allo stesso derivante dal convergere del principio personalista di cui all'art. 2 e del principio di eguaglianza sostanziale di cui all'art. 3, secondo comma, sia consentito rinviare a Passaglia 2014 (spec. p. 13 ss.).

22. La configurazione del diritto di accesso a Internet alla stregua di un diritto sociale trova ampie conferme in dottrina. Sulla tematica, si possono ricordare, oltre a Tanzarella 2013, e al precitato lavoro incentrato sull'impatto del PNRR (Cocchiara 2023, p. 188 ss.), gli scritti nei quali si è commentata la proposta di inserimento di un art. 34-*bis* della Costituzione, in tema di accesso a Internet: cfr., in particolare, Allegri 2021; d'Ippolito 2021; Tanzarella 2021.

darsi, per gli individui, benefici misurabili alla luce dell'art. 3, secondo comma, della Costituzione.

Il fulcro di questa misurazione risiede nell'equazione secondo cui la riduzione dei divari digitali, che concretizza l'incremento delle potenzialità di accesso alle tecnologie, è *di per sé* un beneficio per l'individuo, giacché si pone come una concretizzazione di quell'imperativo di eguaglianza sostanziale che è, a sua volta, funzionale al pieno sviluppo della personalità per l'insieme dei consociati.

Sulla scorta dell'equazione che si è appena delineata, l'analisi dell'efficacia dell'allocazione delle risorse pubbliche viene condotta, essenzialmente, in termini di *quantum*, nel senso che l'unica vera incognita delle azioni intraprese consiste nel grado di *redditività* dell'investimento economico rispetto all'entità della riduzione dei divari digitali. Il presupposto resta comunque quello secondo cui, se l'intervento posto in essere ha un minimo di logica, si assiste a una qualche riduzione, magari anche minima, di almeno uno dei divari e, *dunque*, a un beneficio per gli individui.

Lo sviluppo delle tecnologie richiede, però, un vaglio critico ulteriore, concernente proprio il presupposto: non è probabilmente più il caso di dare per acquisito il fatto che rendere più agevole l'utilizzo delle nuove tecnologie, nella forma della riduzione di un divario digitale, sia indice in sé e per sé di una meritevolezza dell'azione in riferimento alla garanzia del principio personalista. In altri termini, l'atteggiamento positivo nei confronti delle nuove tecnologie che ha animato i primi decenni della rivoluzione digitale richiede ormai una revisione, sulla scorta della quale subordinare l'impegno alla diffusione della loro fruizione a una serie di azioni parallele che assicurino, come minimo, la loro non-nocività.

Solo per fare l'esempio più banale, al fine di giustificare azioni (e risorse impegnate) per promuovere l'accesso a Internet, i pubblici poteri non possono trascurare il loro compito primario di trovare forme di disciplina del fenomeno Internet che prendano in adeguata considerazione la sua struttura tecnologica, onde riuscire a prevenire (e possibilmente a evitare) la "dittatura dell'algoritmo"[23] o, comunque, quegli strumenti, che l'intelligenza artificiale sta rapidamente moltiplicando, attraverso i quali gli utenti della Rete, nell'esercizio apparente della loro libertà di navigazione, divengono in realtà soggetti a un penetrante controllo delle loro condotte e a una diffusa influenza esercitata sulle loro menti[24].

Trattare *funditus* del tema porterebbe lontano rispetto all'oggetto di queste pagine, ma almeno un accenno doveva essere fatto, proprio per restituire l'idea della complessità crescente che connota l'impegno contro le nuove esclusioni sociali su base tecnologica. Una complessità che non si alimenta solo di limitatezza di risorse economiche, ma che cresce anche a causa dell'attuale carenza di risorse regolative di fenomeni sempre più difficili da governare[25].

3. Il diritto a non utilizzare le nuove tecnologie

Durante la pandemia, l'essenzialità delle nuove tecnologie ai fini del mantenimento di una parvenza di socialità e del perdurare di servizi pubblici è stata talmente evidente che qualunque enfatizzazione nel porla in risalto non poteva non apparire retorica.

Proprio nel momento in cui si constatava la centralità delle nuove tecnologie come asse portante della società[26], peraltro, acquisiva una luce sempre meno fioca l'altro lato della medaglia, e cioè quella dei rischi in termini di esclusione sociale insiti nell'evoluzione tecnologica: se la società nella pandemia viveva in buona misura grazie alle nuove tecnologie, si veniva a creare un solco che poteva risultare incolmabile tra la società della pandemia e gli esclusi. Questo ha indotto un diverso modo di approcciarsi ai divari digitali, per i quali la prospettiva di analisi, più che mutare in senso proprio, si è

23. L'espressione è divenuta, ormai, di uso corrente, grazie soprattutto a Steiner 2013, e, in Italia, a Rodotà 2014 (spec. p. 33 ss.).

24. Sul tema, sia consentito, di nuovo, riferirsi a considerazioni già svolte: cfr. Passaglia 2020 (spec. p. 47 ss.).

25. Nella dottrina italiana, l'inquadramento normativo della Rete è stato analizzato, in particolare, da De Minico 2012; più di recente, v. De Minico 2022. Con particolare riguardo alle problematiche legate alla transnazionalità del fenomeno, v. Pollicino–Bassini 2014 e Conti 2021.

26. Cfr. Frosini 2020.

allargata: in altri termini, i divari digitali non sono stati identificati più soltanto come quegli ostacoli da colmare per generalizzare l'accesso alle nuove tecnologie[27]; i divari digitali sono diventati *anche* i motori di esclusioni sociali che l'irrinunciabilità delle tecnologie (durante la pandemia) e l'abitudine alle tecnologie (subito dopo) hanno acuito fino a produrre una vera e propria emergenza.

È in questo contesto che la visione positiva dell'impegno a colmare i divari digitali è stata affiancata dalla visione negativa (*rectius*, realista) dell'impossibilità di colmarli integralmente. In questa seconda lettura, però, il riconoscimento del diritto di accesso alle nuove tecnologie è apparso come insufficiente, in quanto svuotato di contenuti, almeno per quella parte dei soggetti più deboli destinati a restare tali anche dopo un'eventuale azione dei pubblici poteri di rimozione di divari digitali.

Non può allora definirsi un caso che, negli anni più recenti, sia andata crescendo, in dottrina, l'attenzione per una nuova situazione soggettiva, potenzialmente identificabile nel diritto a *non* utilizzare le nuove tecnologie, anch'esso declinato, come il suo versante positivo, principalmente come diritto a non utilizzare Internet[28].

Trattasi di un diritto di non agevole definizione[29], se non altro perché, a ben vedere, racchiude in sé due fattispecie tra loro piuttosto lontane, per fondamenti e per effetti.

Il diritto a non utilizzare Internet e le nuove tecnologie può essere costruito, innanzi tutto, come riflesso negativo della libertà di accesso: al sussistere della possibilità di utilizzo, il soggetto può decidere di astenersi, rinunciando ai benefici che la tecnologia gli assicura, magari per privilegiare altre esigenze o anche altri diritti, come ad esempio quello alla protezione dei dati personali, che in qualunque caso di connessione subisce inevitabilmente una più o meno consistente compressione. Il fondamento risiede precisamente nell'autodeterminazione del singolo, cui – in ipotesi – non può essere imposto quel determinato *facere* consistente nell'accedere a Internet[30]. Il tema è certamente di grande interesse sul piano teorico, ma il suo impatto con riguardo ai rischi di esclusione sociale è, di contro, assai contenuto (per non dire del tutto trascurabile), giacché il diritto di rinunciare all'utilizzo postula che l'esclusione sociale non ci sia, perché l'accesso sarebbe teoricamente possibile, quindi se esso non si produce è soltanto per un atto di volizione del soggetto.

Ben più rilevante, ai presenti fini, è la diversa fattispecie che si presenta quando l'individuo non sia in grado di accedere a Internet. Una fattispecie che, come si è detto, è ineliminabile, proprio perché sono i divari digitali a non esserlo, almeno allo stadio attuale dello sviluppo tecnologico[31]. Una siffatta constatazione conduce a delineare una situazione – per certi versi paradossale, ma tutt'altro che irrealistica – nella quale le nuove tecnologie, per il fatto di non essere alla portata di tutti, da strumento di sviluppo delle potenzialità dell'individuo e di ausilio all'esercizio dei suoi diritti, si

27. Con riferimento al diritto di accesso a Internet nel contesto della pandemia, v. Bosco 2020; Lotta 2020; Valvo 2023.

28. Tra i primi autori a sollevare la tematica inerente alla configurabilità di un diritto a non utilizzare Internet ("or, more broadly, (new) technologies"), v. Kloza 2021; Kloza 2024. Sul tema, v. anche Popa Tache–Săraru–Kouroupis 2024, nonché, volendo, Passaglia 2022. Per una disamina più compiuta del diritto in questione, con analisi svolte da molteplici punti di vista, v. il recentissimo Kloza–Kużelewska–Lievens–Verdoodt 2025.

29. In ordine a una ricostruzione delle diverse possibili definizioni di questo diritto, ci si permette un'ulteriore autocitazione: v., anche per ulteriori riferimenti bibliografici, Passaglia 2025.

30. In questa prospettiva, Popa Tache–Săraru–Kouroupis 2024 (p. 187 ss.), propongono un parallelismo tra il diritto a non utilizzare Internet e il diritto di rifiutare l'istruzione.

31. Probabilmente, un superamento pressoché compiuto di tutti i divari potrebbe essere ipotizzabile solo in base a evoluzioni tanto significative quanto distopiche del transumanesimo, tali da rendere qualunque individuo "naturalmente" connesso. La circostanza stessa che si prospetti una tale evenienza, anche se solo per escluderla, è indice di quanto si stia sviluppando il tema del transumanesimo, il quale sta non a caso conoscendo, negli ultimi tempi, un interesse crescente anche in dottrina: cfr., di recente, in italiano, Bonito–Carrara 2024.

trasformano in catalizzatori di diseguaglianza, vettori di esclusioni sociali nuove o più acute.

La constatazione potrebbe forse dischiudere una qualche velleità luddista, che tuttavia non avrebbe alcun senso, né – come è chiaro – storicamente, né – per quanto qui interessa – da un punto di vista giuridico: onde arginare il paradosso suddetto, infatti, potrebbe venire in rilievo proprio il riconoscimento di un diritto a non usare le nuove tecnologie. In quest'ottica, un tale diritto non avrebbe alcuna attinenza con un assurdo rifiuto del progresso, ponendosi semmai come clausola di salvaguardia in favore di tutti coloro che il progresso finisse per "lasciare indietro".

In che cosa concretamente si sostanzi questa clausola di salvaguardia può essere indicato facendo ricorso a una vicenda prodottasi in Belgio, ormai vari anni fa, e inerente all'esercizio di un diritto non comprimibile (in quando presupposto di un dovere insopprimibile), quale quello di avere la possibilità di conoscere il diritto positivo (*scil.*, al fine di poterlo rispettare). Il legislatore aveva riformato, nel 2002, la disciplina della pubblicazione del *Moniteur belge*, limitando la stampa dei fogli ufficiali a sole tre copie cartacee oltre a quelle richieste in abbonamento. Era stata adita la (allora ancora) *Cour d'arbitrage*, che aveva sottolineato come una tale disciplina producesse l'effetto di rendere impossibile la conoscenza del diritto positivo in vigore a "un nombre important de personnes"; la conseguente incostituzionalità era stata pronunciata, in particolare, alla luce degli effetti pregiudizievoli discendenti dall'assenza di adeguati provvedimenti di accompagnamento volti a garantire comunque l'accesso ai fogli ufficiali a beneficio delle categorie di persone prive della possibilità di accedere a Internet[32]. La decisione aveva dato luogo a una nuova riforma che, nel 2005, aveva introdotto, tra l'altro, previsioni dirette ad agevolare la consultazione del *Moniteur belge* da parte delle categorie ritenute tecnologicamente svantaggiate. Tra le modifiche apportate, oltre all'introduzione di una quarta copia cartacea e di una copia in microfilm, aveva assunto una speciale importanza la previsione in base alla quale era divenuto possibile ottenere, a prezzo di costo, una copia degli atti pubblicati, individuabili anche attraverso un servizio ausiliario prestato via telefono che era stato messo a disposizione gratuitamente. Grazie alle alternative approntate all'accesso a Internet, il giudice costituzionale, nuovamente adito, aveva stavolta ritenuto la nuova disciplina conforme alla Costituzione[33].

Provando a trarre induttivamente indicazioni di ordine generale dalla vicenda appena ricordata, pare che possa porsi il principio secondo cui, persistendo soggetti impossibilitati a fruire delle nuove tecnologie per motivi indipendenti dalla loro volontà, le nuove tecnologie non possono sostituirsi alle forme tradizionali di esercizio di diritti, ma possono a esse soltanto *affiancarsi*, dovendo restare effettivamente attivabile l'opzione che eviti l'accesso a Internet e a quelle tecnologie che siano più idonee a creare nuove o maggiori esclusioni.

Così posto il principio, non si può escludere che sussistano dei casi di obbligo di utilizzo delle nuove tecnologie, ma l'esistenza di un diritto di segno opposto vale a ridurre al massimo la ricorrenza di fattispecie di obbligo, confinandole, in definitiva, all'interno di tre grandi tipologie.

La prima è quella di obblighi di utilizzo finalizzati all'esercizio di condotte che siano ovviamente lecite, ma alle quali l'ordinamento non riconosca una particolare meritevolezza, tanto da accettare che da esse possano essere escluse categorie di soggetti, sul presupposto che dovrà essere cura di coloro che intendano esercitare tali condotte il porsi nelle condizioni di farlo[34].

La seconda tipologia è quella di imposizioni che si rivolgano, non già alla generalità dei consociati, bensì a soggetti identificati o identificabili, per i quali si possano postulare conoscenze

32. *Cour d'arbitrage, arrêt* n. 106/2004, del 16 giugno 2004.

33. *Cour d'arbitrage, arrêt* n. 10/2007, del 17 gennaio 2007. Per qualche dettaglio ulteriore sulla vicenda descritta, sia consentito rinviare a Passaglia 2014 (p. 35 ss.).

34. Un evento sportivo (specie se c.d. "minore") che sia trasmesso soltanto su Internet non può certo dar luogo a una pretesa di trasmissione anche su supporti più tradizionali, stante la carenza di un sufficiente grado di tutela offerta dall'ordinamento. Altro discorso potrebbe farsi per i grandi eventi sportivi, relativamente ai quali si potrebbe forse ipotizzare una estensione. Ciò posto in termini teorici, si tratterebbe comunque di stabilire, caso per caso, il grado di importanza del singolo evento.

informatiche sufficienti a giustificare l'esistenza di un obbligo[35].

La terza e ultima tipologia attiene alle situazioni di emergenza, che, in quanto tali, sono idonee a far saltare i termini dei bilanciamenti che sono stati sopra suggeriti. La lunga parentesi della pandemia da Covid-19 ne è un esempio emblematico, nella misura in cui ha imposto il ricorso alle nuove tecnologie in molti ambiti (dal diritto all'istruzione al diritto al lavoro, passando da quello alla salute e da molti altri) nei quali, in condizioni normali, le alternative "tradizionali" risultano imprescindibili. Ma si tratta, appunto, di situazioni assolutamente eccezionali, nelle quali anche il diritto a non usare le nuove tecnologie, come molti altri diritti, può trovarsi legittimamente compresso entro confini più ristretti di quelli che gli sono (o gli debbono essere) per solito propri.

4. Un'osservazione conclusiva

Le considerazioni che si sono svolte in questo lavoro sono ben lungi dal potersi definire compiute. Sono, anzi, assai provvisorie, trattandosi per lo più di un inventario di problemi su cui si dovrà certamente ritornare. La provvisorietà, peraltro, è strettamente legata anche alla fase di transizione che stanno vivendo le società tecnologicamente più avanzate, esposte alla tensione sempre più forte tra la propensione verso lo sviluppo tecnico-scientifico e il pericolo che proprio questo sviluppo, ingenerando una segmentazione sociale progressivamente crescente, renda complesso il mantenimento di una coesione sociale sufficiente.

Il passaggio dal perseguimento dell'obiettivo di estendere a tutti la fruizione delle nuove tecnologie alla consapevolezza dell'impossibilità di farlo è un momento essenziale nell'ottica di ripensare, anche sul versante prettamente sociale, l'approccio alla tecnologia. Un approccio più critico e consapevole, nel quale una visione dei problemi a spettro più ampio ponga in relazione, in maniera più efficace, il progresso tecnico-scientifico con la protezione degli individui e in special modo degli individui più vulnerabili, onde scongiurare il rischio che il progresso tecnologico si riverberi in un arretramento della giustizia e dell'inclusione sociali.

In questa dinamica, le istituzioni sono destinate a svolgere un ruolo assolutamente centrale e insostituibile. In un'epoca che si vuole sovente orientata alla marginalizzazione dell'intervento pubblico e alla critica delle capacità regolative dei pubblici poteri, forse la lotta contro le esclusioni sociali derivanti dalle tecnologie può rappresentare, magari in forma di sineddoche o fors'anche di embrione, l'emergere di nuovi paradigmi.

Riferimenti bibliografici

M.R. Allegri (2021), *Il diritto di accesso a Internet: profili costituzionali*, in "MediaLaws", 2021, n. 1

G. Arconzo (2020), *I diritti delle persone con disabilità. Profili costituzionali*, FrancoAngeli, 2020

M. Altimari (2021), *L'effettività del diritto alla disconnessione: una sfida per il diritto del lavor*o, in "Rivista italiana di informatica e diritto", 2021, n. 2

C. Bonito, A. Carrara (a cura di) (2024), *Il transumanesimo. Una sfida antropologica alla scienza e alla fede*, Mimesis, 2024

F.M. Bosco (2020), *Digital divide e Covid-19: torna il diritto di accesso ad Internet*, in "MediaLaws. Law and Policy of the Media in a Comparative Perspective", 7 maggio 2020

35. È quanto si produce, ad esempio, con l'obbligo imposto a molti lavoratori (dipendenti o autonomi) di utilizzare Internet e nuove tecnologie per motivi professionali: in tal caso, il diritto a non utilizzare Internet non può essere invocato allorché il fatto di opporre una impossibilità sia incompatibile con lo svolgimento delle mansioni o della professione. Così, il docente, per quanto possa trovare afflittiva la compilazione di registri delle lezioni in forma elettronica, non potrà – salvi casi eccezionali – rifiutarsi di farlo. L'elenco delle situazioni di analogo tenore sarebbe ovviamente molto lungo.

F. Camillieri (2024), *Rassegna sul tema dell'accesso ad Internet in carcere a livello comparato: tra riconoscimenti teorici e difficoltà pratiche*, in "Rivista italiana di informatica e diritto", 2024, n. 1

B. Carotti (2010), *L'accesso alla rete e la tutela dei diritti fondamentali*, in "Giornale di diritto amministrativo", 2010, n. 6

V.G. Cerf (2012), *Internet Access Is Not a Human Right*, in "The New York Times", 4 January 2012

E. Cocchiara (2023), *Il divario digitale nel PNRR: la garanzia del diritto sociale di accesso ad Internet*, in "Forum di Quaderni costituzionali – Rassegna", 2023, n. 2

G.L. Conti (2021), *La lex informatica*, in "Osservatorio sulle fonti", 2021, n. 1

S. da Empoli (2023), *Il percorso di sviluppo delle competenze digitali in Italia e l'impatto dell'innovazione sull'istruzione*, Indagine conoscitiva sull'impatto della digitalizzazione e dell'innovazione tecnologica sui settori di competenza della VII Commissione della Camera dei deputati (audizione 3 maggio 2023)

S. da Empoli (2021), *Un approccio economico al diritto di accesso a Internet: verso una revisione del servizio universale*, in "MediaLaws", 2021, n. 1

E. De Fort (1995), *Scuola e analfabetismo nell'Italia del '900*, il Mulino, 1995

T. De Mauro (1963/2011), *Storia linguistica dell'Italia unita*, Laterza, 2011

G. De Minico (2022), *Le fonti al tempo di Internet: un personaggio in cerca d'autore*, in "Osservatorio sulle fonti", 2022, n. 1

G. De Minico (2012), *Internet. Regola e anarchia*, Jovene, 2012

G. d'Ippolito (2021), *Il diritto di accesso ad Internet in Italia: dal 21(-bis) al 34-bis*, in "MediaLaws", 2021, n. 1

G. Formici (2023), *Access denied: gli* Internet shutdowns *alla prova del diritto. Spunti di riflessione a partire dalla giurisprudenza della* Supreme Court *indiana*, in "DPCE Online", 2023, n. 1

T.E. Frosini (2020), *Internet ai tempi del coronavirus*, in "Diritto di Internet", 2020, n. 2

T.E. Frosini (2011), *Il diritto costituzionale di accesso a Internet*, in "Rivista dell'Associazione italiana dei costituzionalisti", 2011, n. 1

D. Kloza (2024), *The right not to use the internet*, in "Computer Law & Security Review", vol. 52, 2024

D. Kloza (2021), *It's All About Choice. The Right Not to Use the Internet*, in "Völkerrechtsblog", 29 November 2021

D. Kloza, E. Kużelewska, E. Lievens, V. Verdoodt (eds.) (2025), *The Right Not to Use the Internet. Concept, Contexts, Consequences*, Routledge, 2025

C. Lotta (2020), *Un nuovo diritto al tempo del Covid-19? Accesso a Internet e* digital divide, in "Rivista del Gruppo di Pisa", 2020, n. 2

N. Lucchi (2011), *Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression*, in "Cardozo Journal of International and Comparative Law", vol. 19, 2011, n. 3

N. Lucchi (2010), *La legge "Création et Internet". Le censure del* Conseil constitutionnel *e lo Stato di diritto*, in "Quaderni costituzionali", 2010, n. 2

A. Pace (2004), *I progetti "PC ai giovani" e "PC alle famiglie": esercizio di potestà legislativa esclusiva statale o violazione della potestà regionale residuale?*, in "Giurisprudenza costituzionale", 2004, n. 5

P. Passaglia (2025), *An attempt to conceptualise the right to access the Internet and its impact on the right not to use it*, in D. Kloza, E. Kużelewska, E. Lievens, V. Verdoodt (eds.), "The Right Not to Use the Internet. Concept, Contexts, Consequences", Routledge, 2025

P. Passaglia (2022), *Behind the Curtain: Questioning the Right to Access the Internet, in Search of Definitions (and Conditions)*, in "Völkerrechtsblog", 17 ottobre 2022

P. Passaglia (2020), *Ancora sul fondamento costituzionale di* Internet*. Con un ripensamento*, in "*Liber Amicorum* per Pasquale Costanzo. Diritto costituzionale in trasformazione. Tomo I – Costituzionalismo, reti e intelligenza artificiale", Collana di Studi di Consulta Online, 2020

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

P. Passaglia (2009), *L'accesso ad Internet è un diritto (il Conseil constitutionnel francese dichiara l'incostituzionalità di parte della c.d. "legge anti file-sharing")*, in "Il Foro italiano", 2009, n. 10

M. Pietrangelo (a cura di) (2011), *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.G. Pizzetti (2008), *Il progetto "PC ai giovani" nel quadro della promozione dell'eguaglianza digitale da parte dello Stato e delle Regioni*, in "federalismi.it", 2008, n. 12

O. Pollicino, M. Bassini (2014), *The Law of the Internet between Globalisation and Localisation*, in M. Maduro, K. Tuori, S. Sankari (eds.), "Transnational Law. Rethinking European Law and Legal Thinking", Cambridge University Press, 2014

C.E. Popa Tache, C.S. Săraru, K. Kouroupis (2024), *Different perspectives concerning the right not to use the internet and some analogies with education*, in "European Journal of Privacy Law & Technologies", 2024, n. 1

P. Ridolfi (a cura di) (2002), *I disabili nella società dell'informazione*, FrancoAngeli, 2002

S. Rodotà (2014), *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, 2014

T. Sica (2022), *Disabilità e accesso a internet*, in "Diritto Mercato Tecnologia", 2022

C. Steiner (2013), *Automate This. How Algorithms Took Over Our Markets, Our Jobs, and the World*, Portfolio, 2013

P. Tanzarella (2021), *L'accesso a Internet è fondamentale, ma è davvero un diritto (fondamentale)?*, in "MediaLaws", 2021, n. 1

P. Tanzarella (2013), *Accesso a Internet: verso un nuovo diritto sociale?*, in E. Cavasino, G. Scala, G. Verde (a cura di), "I diritti sociali dal riconoscimento alla garanzia. Il ruolo della giurisprudenza", Atti del Convegno annuale del Gruppo di Pisa, Trapani 8-9 giugno 2012, Editoriale Scientifica, 2013

L.A. Valvo (2023), *Il diritto di accesso ad Internet alla prova del Covid-19*, in E. Benedetti, A. Piacquadio, L. Fabrizi, (a cura di), "Scritti in onore di Gian Luigi Cecchini. Liber Amicorum", Giuffrè, 2023

G. Votano (2009), *Internet fra diritto d'autore e libertà di comunicazione: il modello francese*, in "Diritto dell'informazione e dell'informatica", 2009, n. 3

I. Zoppoli (2023), *Il diritto alla disconnessione nella prospettiva europea: una* road map *per le parti sociali*, in "federalismi.it", 2023, n. 1

RIVISTA ITALIANA
DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0239 • articolo sottoposto a peer review • pubblicato in anteprima il 1 ott. 2025

Alberto Quintavalla

Protezione dei diritti umani e intelligenza artificiale: un'analisi critica del regolamento europeo sui prodotti a duplice uso

Questo testo si propone di analizzare l'adeguatezza della protezione dei diritti umani nel contesto del regolamento europeo sui prodotti a duplice uso. Dopo aver esaminato come il legislatore europeo abbia progressivamente integrato nella regolamentazione sui prodotti a duplice uso considerazioni in materia di diritti umani, il testo esplora come rimangano certe limitazioni nel quadro normativo attuale. In particolare, viene messa in discussione la capacità della normativa europea di garantire la certezza del diritto, essenziale per una applicazione uniforme e rispettosa dei diritti fondamentali. In tal modo, questo studio mira a contribuire a una comprensione più profonda delle possibili interazioni che emergono a livello normativo circa la protezione dei diritti umani e la politica europea commerciale comune in materia di prodotti a duplice uso e nel contesto della intelligenza artificiale.

Diritti umani – Intelligenza artificiale – Prodotti a duplice uso – Unione europea

Human rights protection and artificial intelligence: a critical analysis of the european regulation on dual-use items

This article aims to assess the effectiveness of human rights protection within the framework of EU regulation on dual-use items. It begins by exploring how the European legislator has progressively integrated human rights considerations into the regulation of these items. The article then addresses the ongoing limitations within the current regulatory landscape. In particular, it examines the ability of European legislation to ensure legal certainty, which is essential for fostering a consistent application that upholds human rights. Consequently, this study enhances our understanding of the interplay between human rights protection and common European trade policy.

Human rights – Artificial intelligence – Dual use items – European Union

L'Autore è Associate Professor in Innovation of Public Law presso l'Erasmus School of Law (Erasmus University Rotterdam) e Co-Director of the Erasmus Center of Law and Digitalization

Questo contributo fa parte della sezione monografica *Le due facce della rivoluzione digitale, tra emergenze e tecnologie* dual-use, a cura di Paolo Passaglia

1. Introduzione

Il crescente dispiegamento di sistemi di intelligenza artificiale sta cambiando la nostra società non solo per gli aspetti civili ma anche quelli militari e, quindi, di guerra. Un classico esempio è l'uso sempre più frequente di armi autonome nelle operazioni militari per la loro migliore performance rispetto alle armi tradizionali in termini di prestazioni ed efficienza. L'uso improprio dei sistemi di intelligenza artificiale, tuttavia, non si limita alle armi autonome in conflitti militari. Nel 2023 il governo del Regno Unito ha riconosciuto che l'intelligenza artificiale generativa può aumentare la velocità, la portata e la sofisticazione degli attacchi che possono essere messi in atto da attori pubblici e privati con intenti malevoli[1]. Osservazioni analoghe relative all'uso della stessa o di altri tipi di intelligenza artificiale sono state condivise da diversi Stati e entità sovranazionali[2].

È in questo contesto che la tecnologia dell'intelligenza artificiale, definibile come una categoria ampia comprendente una vasta serie di applicazioni diverse[3], ha reso ancora piú attuale la discussione sui prodotti a duplice uso. I cosiddetti "prodotti a duplice uso" sono considerati beni, software e tecnologie che possono essere utilizzati sia per applicazioni civili che militari. Questi prodotti sono solitamente progettati per fornire un evidente beneficio in ambito civile, ma allo stesso tempo potrebbero essere facilmente applicati impropriamente in un contesto bellico o, similmente, per perpetrare gravi violazioni dei diritti umani e del diritto umanitario internazionale. Ad esempio, l'uso di modelli basati su agenti (i cosiddetti "agent-based model" di intelligenza artificiale)[4] è necessario per sviluppare veicoli a guida autonoma ma, allo stesso tempo, può diventare funzionale per lo sviluppo di armi letali autonome.

1. UK Government, *Research and analysis. Safety and security risks of generative artificial intelligence to 2025 (Annex B)*, 2025.
2. Cfr., ad es., Amnesty International 2020; UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Surveillance and Human Rights*, UN Doc A/HRC/41/35 (28 May 2019), par. 2.
3. Varie definizioni sono state fornite per quanto concerne il termine (sistema di) intelligenza artificiale. Per esempio, secondo il legislatore europeo nell'AI Act, un sistema di intelligenza artificiale viene definito come "un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali". Sulla base di tale definizione, un sistema di intelligenza artificiale racchiude una svariata serie di applicazioni, da (ad es.) sistemi generativi a (ad es.) sistemi predittivi.
4. I modelli basati su agenti sono entità decisionali autonome che percepiscono il loro ambiente, prendono decisioni in base alle loro percezioni e poi agiscono per raggiungere obiettivi specifici.

Infatti, bisogna osservare come l'avvento dell'intelligenza artificiale possa porre rischi ancora più gravi rispetto alle tecnologie tradizionali quando si tratta di tecnologie nel contesto di prodotto a duplice uso. L'intelligenza artificiale si basa su software, il che ne consente una facile diffusione e, possibilmente, un potenziale furto da parte di attori che hanno finalità ostili. Come evidenziato in varie ricerche, le tecnologie di intelligenza artificiale sviluppate in ambito civile possono offrire potenti capacità ad applicazioni militari[5]. In particolare, questo rischio si materializza ove si faccia riferimento a un tipo specifico di intelligenza artificiale, ossia quella dei cosiddetti modelli fondativi (*foundational models*) per la loro facile applicabilità e scalabilità in molteplici contesti[6].

L'Unione europea ha cercato di affrontare i rischi connessi ai prodotti a duplice uso adottando un regolamento nell'ambito della politica commerciale comune[7]. Il regolamento europeo è stato notevolmente rivisto nel corso degli anni e, alla fine, ha riguardato anche la tecnologia dell'intelligenza artificiale. Questo sviluppo normativo mirava principalmente a garantire che il commercio e gli investimenti connessi all'industria dell'intelligenza artificiale non facilitassero l'uso improprio di tale tecnologia. In altre parole, l'inclusione dell'intelligenza artificiale nel regolamento sui prodotti a duplice uso può essere attribuita agli sforzi normativi posti in essere da parte dell'Unione europea per rendere l'intelligenza artificiale una tecnologia più affidabile.

Difatti, le "Linee guida etiche per un'intelligenza artificiale affidabile" adottate dalla Commissione europea poggiano su tre diversi pilastri, in cui la dimensione giuridica si affianca a quella etica e a quella tecnica[8]. Per quanto riguarda la dimensione giuridica, l'Unione europea ha progressivamente adottato una serie di atti normativi volti a plasmare il tradizionale approccio basato sul rischio attorno all'idea di assicurare un approccio antropocentrico (ossia di "human centric AI"). Parte ed espressione di questi sforzi normativi è sicuramente l'adozione del regolamento sull'intelligenza artificiale, la cui finalità "di promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea" viene esplicitata nel primo considerando[9].

Il legislatore europeo mira in tal modo ad assicurare che lo sviluppo dell'intelligenza artificiale avvenga non solo in modo che i rischi possano essere evitati ma che lo sviluppo sia, tra le altre cose, "al servizio delle persone, nel rispetto della dignità umana e dell'autonomia personale"[10]. Questi valori sono essenziali e forniscono supporto all'idea che lo sviluppo dell'intelligenza artificiale non possa prescindere dal rispetto dei diritti umani[11]. Ed è proprio alla luce di queste considerazioni

5. Trusilo–Danks 2024, pp. 2-3.
6. Horowitz 2019.
7. Regolamento (UE) 2021/821 del Parlamento europeo e del Consiglio del 20 maggio 2021 che istituisce un regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso (rifusione). Per un commentario sul regolamento, v. Fruscione 2022.
8. Commissione europea, *Creare fiducia nell'intelligenza artificiale antropocentrica*, COM(2019) 168. Questo gruppo di esperti ad alto livello sull'intelligenza artificiale (AI HLEG) fu nominato dalla Commissione nel 2019 per elaborare (sette) principi etici per una intelligenza artificiale affidabile.
9. Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828.
10. V. Commissione europea, *Creare fiducia nell'intelligenza artificiale antropocentrica*, COM(2019) 168, p. 2.
11. Per esempio, il valore della dignità umana è solitamente tradotto nella sua dimensione prettamente giuridica attraverso il gergo dei diritti umani: qualsiasi studioso di diritti umani sarebbe d'accordo sul fatto che la dignità umana è il fondamento della normativa in materia di protezione dei diritti umani. Sul punto, v. Donnely 1982; Donnelly 2013.

che l'integrazione di considerazioni inerenti ai diritti dell'uomo non si limitano alla normativa che stabilisce regole armonizzate sull'intelligenza artificiale, ossia l'AI Act, ma giocano un ruolo importante anche in altre discipline che possono riguardare l'intelligenza artificiale come la recente modifica della regolamentazione dei prodotti a duplice uso.

Pertanto, è importante indagare in che misura la protezione dei diritti umani offerta dal regolamento sui prodotti a duplice uso possa essere considerata adeguata per garantire un'intelligenza artificiale affidabile, in particolare per quanto riguarda la dimensione di certezza del diritto. Il resto di questo contributo è strutturato come segue. Il secondo paragrafo si sofferma sul modo in cui le considerazioni inerenti ai diritti umani sono state inserite all'interno della regolamentazione a livello europeo. Solo una volta che questa indagine è stata completata, il terzo paragrafo del contributo può valutare come il quadro attuale fornisca una normativa che si regge precipuamente sulla discrezionalità assegnata ai singoli Stati membri. Di conseguenza, il quarto paragrafo pone il quesito se si possa considerare che la normativa europea sui prodotti a duplice uso rispetti la dimensione di certezza del diritto all'interno del territorio europeo.

2. La regolamentazione europea sui prodotti a duplice uso: una maggiore attenzione alle considerazioni in materia di diritti umani?

L'Unione europea ha riconosciuto la necessità di prevenire l'uso improprio dei prodotti a duplice uso a partire dai primi anni Novanta del secolo scorso. Il primo atto normativo europeo adottato a questo riguardo è stato il Regolamento (CE) n. 3381/94 il quale era volto a istituire controlli armonizzati sulle esportazioni di beni a duplice uso[12]. L'ambito di applicazione di quel regolamento, tuttavia, era limitato ai controlli sulle esportazioni di beni materiali, non comprendendo quindi i software o le tecnologie. È solo con il Regolamento (CE) n. 1334/2000 che l'ambito di applicazione della normativa europea viene esteso al software e alle tecnologie, così sostituendo l'espressione "beni a duplice uso" con "prodotti a duplice uso"[13].

Tale quadro normativo è stato poi riformulato significativamente con l'entrata in vigore del Regolamento (CE) n. 428/2009 in cui si istituisce un regime comunitario di controllo delle esportazioni, del trasferimento, dell'intermediazione e del transito di prodotti a duplice uso e, per la prima volta, si fa riferimento a considerazioni relative ai diritti umani[14]. In particolare, ai sensi dell'articolo 8 del regolamento, viene concessa agli Stati membri la facoltà di "vietare l'esportazione di prodotti a duplice uso" oppure di "imporre per gli stessi [prodotti a duplice uso] un requisito di autorizzazione" per motivi di tutela dei diritti umani. Le misure che vengono così adottate dagli Stati membri devono poi essere notificate alla Commissione europea e, da quest'ultima, pubblicate sulla Gazzetta ufficiale dell'Unione a fini informativi.

L'inserimento di considerazioni inerenti ai diritti umani all'articolo 8 del regolamento, tuttavia, non riesce a contribuire ad uno sviluppo di un quadro normativo adeguato per combattere l'uso improprio dei prodotti a duplice uso in termini di protezione di sicurezza umana. Specificatamente, la Commissione europea esprime la necessità di rivedere il suddetto regolamento enfatizzando come le minacce derivanti dai rapidi progressi tecnologici rendano urgente una revisione del regolamento[15]. Per esempio, nel 2014, la Commissione

12. Regolamento (CE) n. 3381/94 del Consiglio, del 19 dicembre 1994, che istituisce un regime comunitario di controllo delle esportazioni di beni a duplice uso.
13. Regolamento (CE) n. 1334/2000 del Consiglio, del 22 giugno 2000, che istituisce un regime comunitario di controllo delle esportazioni di prodotti e tecnologie a duplice uso.
14. Regolamento (CE) n. 428/2009 del Consiglio, del 5 maggio 2009, che istituisce un regime comunitario di controllo delle esportazioni, del trasferimento, dell'intermediazione e del transito di prodotti a duplice uso (rifusione).
15. Si noti che ai sensi dell'articolo 25 del Regolamento 428/2009, la Commissione dovrebbe riesaminare l'attuazione del regolamento ogni tre anni. Per osservazioni circa la pericolosità delle tecnologie a duplice uso cfr. Conclusioni del Consiglio, del 21 ottobre 2013, sul tema "Assicurare il costante perseguimento di un'efficace politica dell'Unione europea per le nuove sfide rappresentate dalla proliferazione delle armi di distruzione di massa (ADM)".

europea sottolinea come la regolamentazione sui prodotti a duplice uso debba evolversi verso l'adozione di un approccio improntato alla "sicurezza umana" in cui la violazione dei diritti umani deve essere parte integrante di tale normativa[16].

Il concetto di "sicurezza umana" – e, con esso, la protezione dei diritti umani – incomincia ad assumere un ruolo sempre più importante nei dibattiti a livello europeo. Infatti, vari studi di organizzazioni non governative dimostrano come le esportazioni autorizzate dall'Unione europea di prodotti a duplice uso, in particolare sotto forma di tecnologie di sorveglianza informatica, hanno direttamente contribuito alle violazioni di diritti umani fondamentali come il diritto alla privacy, la libertà di espressione e la libertà di associazione in diversi paesi del mondo[17].

Sulla base di queste considerazioni, nel 2016, la Commissione europea presenta una proposta per modernizzare e rafforzare i controlli sulle esportazioni di prodotti a duplice uso. La tutela dei diritti umani in quella proposta legislativa diventa uno dei pilastri normativi[18]. In particolare, la proposta mira a fornire una "risposta efficace alle minacce per i diritti umani derivanti dalla esportazione incontrollata dei prodotti a duplice uso"[19]. Tale proposta legislativa subisce però una serie di modifiche nel corso degli anni successivi da parte delle altre istituzione europee coinvolte nel processo legislativo europeo – ossia il Parlamento e il Consiglio. In particolare, l'enfasi sulla protezione in materia di diritti umani è oggetto di un forte dibattito che si apre tra la Commissione europea e il Parlamento, da una parte, e il Consiglio, dall'altra[20]. Inoltre, quest'ultimo vede anche ulteriori disaccordi tra due blocchi contrapposti di Stati membri circa il ruolo che si deve attribuire alle considerazioni in materia di diritti umani quando decidere se esportare prodotti a duplice uso[21].

Pertanto, il regolamento che viene adottato dall'Unione europea dopo un lungo iter legislativo durato cinque anni sembra inquadrarsi come l'esito di un processo di bilanciamento tra due diversi obiettivi: assicurare una normativa armonizzata per i prodotti a duplice uso nell'ambito della politica commerciale comune e, nel contempo, proteggere i diritti umani e il diritto internazionale umanitario a livello mondiale[22]. In questo modo, da un lato, il regolamento costituisce parte integrante della politica commerciale comune dell'Unione europea, che la stessa ha storicamente fortemente promosso parallelamente al processo di integrazione del mercato interno[23]. D'altro canto, l'Unione europea – e, in particolar modo, la Commissione europea e il Parlamento europeo – vogliono enfatizzare come una protezione

16. Commissione europea, *Revisione della politica di controllo delle esportazioni: garantire la sicurezza e la competitività in un mondo in evoluzione*, COM (2014) 244, p. 6.
17. Sul punto v. Amnesty International 2020.
18. Kanetake 2020.
19. Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un regime dell'Unione di controllo delle esportazioni, del trasferimento, dell'intermediazione, dell'assistenza tecnica e del transito di prodotti a duplice uso (rifusione)*, COM(2016) 616, p. 6.
20. Cfr. Consiglio europeo, *Proposal for a for a Regulation of the European Parliament and of the Council Setting Up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items (Recast) – Mandate for Negotiations with the European Parliament*, 2019; Consiglio europeo *New Rules on Trade of Dual-Use Items Agreed*, 2020; Parlamento europeo, *Emendamenti del Parlamento europeo, approvati il 17 gennaio 2018, alla proposta di regolamento del Parlamento europeo e del consiglio che istituisce un regime dell'Unione di controllo delle esportazioni, del trasferimento, dell'intermediazione, dell'assistenza tecnica e del transito di prodotti a duplice uso (rifusione)*, 2018.
21. Sul punto, v. Bromley 2023; Riecke 2023.
22. Cfr. Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un regime dell'Unione di controllo delle esportazioni, del trasferimento, dell'intermediazione, dell'assistenza tecnica e del transito di prodotti a duplice uso (rifusione)*, 2016, pp. 2-3; Commissione europea, *Commercio per tutti verso una politica commerciale e di investimento più responsabile*, COM(2015) 497, pp. 22-23.
23. Jaremba–Kanetake–Koning 2019, p. 2. Sul punto v. Meissner–Urbanski 2022, p. 224.

adeguata dei diritti umani sia diventata una esigenza complementare. La base giuridica su cui si fonda la proposta legislativa della Commissione europea riflette la coesistenza di questi due diversi obiettivi in quanto, nonostante si basi sulla competenza relativa alla politica commerciale comune ai sensi dell'articolo 207 del Trattato sul funzionamento dell'Unione europea, si menziona in modo esplicito che l'intervento europeo è necessario dato che le esportazioni di tecnologie di sorveglianza informatica possono portare alla violazione della Carta dei diritti fondamentali dell'Unione europea.

Inoltre, il fatto che considerazioni in materia di diritti umani siano state fatte presenti non dovrebbe stupire in quanto è la stessa architettura costituzionale europea a richiedere una maggiore integrazione delle stesse nelle politiche commerciali comuni. Specificamente, il combinato disposto dell'articolo 207 del Trattato sul funzionamento dell'Unione europea e dell'articolo 21 del Trattato sull'Unione europea stabilisce come "l'universalità e l'indivisibilità dei diritti dell'uomo e delle libertà fondamentali" deve sempre essere rispettata nell'attuazione delle politiche e le leggi dell'Unione europea in materia di politica commerciale comune.

Le considerazioni inerenti ai diritti umani hanno cosí trovato recepimento nella normativa europea anche se solo a seguito delle successive modifiche al regolamento sui prodotti a duplice uso. Inoltre, tale recepimento non è stato totale. Le proposte originarie della Commissione europea che miravano a offrire una protezione ben più sviluppata in materia di diritti umani sono state affievolite durante l'iter legislativo. La versione finale del regolamento europeo, pertanto, recepisce le considerazioni in materia di diritti umani ma, come si noterà dalla trattazione del successivo paragrafo, lascia un ampio margine di discrezionalità agli Stati membri.

Tale approccio non solo risponde a esigenze di natura prettamente politico-economica, ma si deve leggere alla luce del dettato costituzionale europeo. A tale riguardo, vale la pena sottolineare che né il suddetto articolo 207 né l'articolo 21 del Trattato sull'Unione europea forniscono indicazioni concrete in merito alla misura in cui i diritti umani e le libertà fondamentali debbano essere integrate alle politiche di diritto commerciale comune e di investimento. In altri termini, la decisione su come la protezione dei diritti umani e la politica commerciale comune interagiscano dipende dalla volontà delle istituzioni europee e degli Stati membri chiamati a implementare la normativa europea.

3. Il livello di armonizzazione in materia di regolamentazione di prodotti a duplice uso nel contesto dei diritti umani

L'attuale regolamento europeo non opera come un sistema completamente armonizzato in termini di controlli sulle esportazioni di prodotti a duplice uso. Infatti, tale controllo può essere stabilito sia a livello europeo che a livello nazionale ai sensi dell'articolo 3 del regolamento. In altri termini, il suddetto articolo offre la possibilità di subordinare l'esportazione dei prodotti a duplice uso a quanto statuito a livello europeo (primo paragrafo) o, in secondo luogo, a quanto deciso dagli Stati membri per certe istanze specificamente regolamentate (secondo paragrafo). Secondo il primo paragrafo, l'allegato I contiene un elenco di tutti quei prodotti per i quali è necessario ottenere un'autorizzazione prima dell'esportazione al di fuori del territorio dell'unione doganale europea. Viceversa, nel secondo paragrafo, si offre agli Stati membri una serie di istanze specifiche in cui godono di maggiore discrezionalità. Infatti, il legislatore europeo ha previsto una serie di cosiddette "clausole onnicomprensive" attraverso cui gli Stati membri possono introdurre ulteriori divieti di esportazione o obblighi di autorizzazione per l'esportazione[24].

Ed è proprio nell'ambito di queste clausole onnicomprensive che le considerazioni inerenti ai diritti umani svolgono un ruolo di primo piano. In particolare, gli articoli 5 e 9 del regolamento sottolineano la necessità di istituire un quadro normativo in grado di rispondere tempestivamente a possibili minacce ai diritti umani. Innanzitutto, ai sensi dell'articolo 5, paragrafo 1, le autorità nazionali competenti possono stabilire che sia necessaria un'autorizzazione per l'esportazione di prodotti per la sorveglianza informatica nel caso in cui abbiano informato l'esportatore che tali "prodotti sono o possono essere destinati, in tutto o in parte, a un uso connesso alla repressione interna e/o

24. Il regolamento fa riferimento alle varie possibilità che sono concesse agli Stati membri per introdurre divieti di esportazione o obbligo di autorizzazione ai sensi degli articoli 4, 5, 9 o 10.

all'attuazione di gravi violazioni dei diritti umani o del diritto umanitario internazionale"[25]. In secondo luogo, ai sensi dell'articolo 9, considerazioni inerenti al rispetto dei diritti umani possono costituire per gli Stati membri motivi legittimi per vietare del tutto l'esportazione o per imporre un obbligo di autorizzazione per un qualsiasi prodotto a duplice uso – a differenza dell'articolo 5 che si limita ai prodotti per la sorveglianza informatica. In tal modo, l'articolo 9 consente la creazione a livello di Stato membro di un elenco di prodotti a duplice uso che non possono essere esportati o necessitano di una autorizzazione per l'esportazione.

Inoltre, la normativa europea non si limita a lasciare la decisione sulla valutazione di gravi violazione di diritti umani ai singoli Stati membri, ma sembra attribuire anche una certa responsabilità agli stessi esportatori. Infatti, ai sensi dell'articolo 5, paragrafo 2, gli esportatori hanno un obbligo di notifica all'autorità competente qualora siano a conoscenza del fatto che prodotti di sorveglianza informatica siano destinati alla commissione di gravi violazioni dei diritti umani o del diritto internazionale umanitario[26]. In tal modo, gli esportatori sono in parte chiamati a esercitare un processo di dovuta diligenza tramite un obbligo di comunicazione[27]. Tuttavia, bisogna riconoscere come la disposizione normativa che è stata adottata nel testo finale abbia attenuato significativamente le obbligazioni che erano state previste in capo agli esportatori da parte della Commissione nella proposta originaria a seguito delle preoccupazioni espresse dagli attori privati – in particolare, gli esportatori – che non volevano addossarsi obbligazione che più si addicevano a organi statali[28].

Il quadro normativo risultante permette quindi agli Stati membri (e, in parte, agli esportatori stessi) di godere di un certo margine di discrezionalità quando si tratta di decidere se concedere licenze di esportazione per i prodotti a duplice uso e, in particolar modo, per i prodotti di sorveglianza informatica. Tali licenze di esportazione dipendono, infatti, dal modo in cui gli Stati membri intendono rendere operativo il concetto di gravi violazioni dei diritti umani e del diritto internazionale umanitario[29]. È quindi probabile come, nell'attuale contesto geopolitico, possano emergere notevoli differenze nell'attuazione del regolamento. Non è un caso che, durante l'iter legislativo del regolamento, alcune associazioni abbiano richiesto alle istituzioni europee di specificare quali fossero le violazioni dei diritti umani da considerare così come di indicare una lista di specifici paesi con una storia di violazioni sistematiche di diritti umani[30]. Tale richiesta era stata avanzata precisamente per evitare che emergesse un'eccessiva discrezionalità nella fase di implementazione del regolamento europeo.

Tuttavia, va riconosciuto che l'Unione europea ha tentato di limitare una eterogeneità normativa a livello nazionale adottando una serie di disposizione specifiche all'interno del regolamento. Innanzitutto, lo Stato membro che ha adottato (o modificato) le liste dei controlli nazionali sulle esportazioni è obbligato a notificare tali modifiche alla Commissione europea e agli altri Stati membri[31]. Tale obbligo di segnalazione è finalizzato a fare sì che la Commissione europea possa

25. Bisogna notare come l'articolo 5 del regolamento e, in particolare, l'inciso sulle considerazioni in materia di diritti umani, come originariamente proposto dalla Commissione europea, sia stato oggetto di forti critiche da parte del Consiglio. Nonostante ciò, anche se tale riferimento è rimasto nella versione finale, il suo ambito di applicazione viene fortemente limitato dalle modifiche apportate alla definizione restrittiva di prodotti a sorveglianza informatica. Cfr. Bromley 2024; Van Daalen–Van Hoboken–Rucz 2023.
26. Sarà poi compito dell'autorità nazionale competente di decidere in merito all'opportunità di sottoporre l'esportazione interessata ad autorizzazione.
27. Si noti che per valutare se questo processo sia avvenuto in modo conforme da parte dell'esportatore vanno presi in considerazione alcuni criteri come le dimensioni e la struttura organizzativa.
28. Sul punto cfr. BDI 2016, p. 7; DIGITALEUROPE 2018, p. 2.
29. Di Franco 2022.
30. Kanetake 2020.
31. Articolo 9, paragrafo 2. A tal riguardo, si deve notare come la Commissione europea non sia soggetta ad alcun obbligo analogo ai sensi degli articoli 4 o 5 del regolamento.

procedere alla pubblicazione delle decisioni degli Stati membri circa i controlli nazionali sulle esportazioni, così come la compilazione degli elenchi di controllo nazionali in vigore. In tal modo, questo meccanismo potrebbe indurre gli altri Stati membri ad applicare simili controlli, facilitando così un approccio più armonizzato in tutta l'Unione europea. Similmente, l'articolo 10 consente alle autorità di altri Stati membri di adottare la stessa proibizione o lo stesso requisito di autorizzazione di un altro Stato membro ai propri esportatori.

Inoltre, la Commissione europea ha pubblicato nell'ottobre del 2024 delle linee guida per fornire strumenti – a sua detta – pratici per valutare l'impatto sui diritti umani[32]. In tali linee guida viene fatto riferimento a quelli che sarebbero i diritti umani maggiormente colpiti dai prodotti a sorveglianza informatica. Questi variano dal diritto alla vita privata e alla protezione dei dati, alla libertà di espressione, dalla libertà di associazione e di riunione al divieto di discriminazione. In altri termini, l'attenzione del legislatore europeo si pone quasi esclusivamente su quelle violazioni di diritti civili e politici che vengono generalmente associate all'impatto negativo di tali tecnologie[33]. Contestualmente, si sottolinea come la valutazione sulla gravità della violazione dei diritti umani debba dipendere caso per caso considerando se le eventuali restrizioni siano giustificate in base al principio di proporzionalità[34]. Nella suddetta valutazione, informazioni su gravi violazioni dei diritti umani pubblicate dagli organi competenti delle Nazioni Unite, dell'Unione o del Consiglio d'Europa possono essere utili; tuttavia, non necessarie[35].

Di conseguenza, sebbene il regolamento europeo sui prodotti a duplice uso rientri nell'ambito di applicazione della politica commerciale comune, una dose significativa di poteri normativi (e amministrativi) rimane nelle mani degli Stati membri. Questi sono sì chiamati a consultare le decisioni adottate da altri Stati membri e pubblicate da parte della Commissione europea ma, allo stesso tempo, sono liberi di adottare le decisioni che ritengono opportune, anche quando gli altri Stati membri si siano espressi diversamente. I tentativi concreti da parte dell'Unione europea volti a fornire una maggiore armonizzazione per quanto concerne l'implementazione del regolamento in termini di diritti umani non hanno evitato che l'ultima parola spetti agli Stati membri.

4. Osservazioni conclusive

Il paragrafo precedente dimostra come la normativa europea sui prodotti a duplice uso possa dar luogo ad un'applicazione eterogenea in tutto il territorio europeo quando la possibile violazione di diritti umani deve essere valutata. Di conseguenza, bisogna domandarsi se tale approccio sia sufficientemente adeguato per assicurare uno sviluppo e una diffusione dell'intelligenza artificiale rispettosa dei diritti umani. In altri termini, se l'attuale normativa europea contribuisca a rendere l'intelligenza artificiale una tecnologia affidabile, così come prospettato nelle linee guida adottate dalla Commissione europea.

Innanzitutto, bisogna riconoscere che le recenti modifiche al regolamento sui prodotti a duplice uso sono riuscite a dare una maggior enfasi alla protezione dei diritti umani. Questo è stato fatto tramite un cambiamento della inquadratura stessa del problema normativo legato ai prodotti a duplice uso che il legislatore europeo è andato ad affrontare. In altri termini, il legislatore europeo ha identificato nella normativa in materia di diritti umani e nel diritto internazionale umanitario il quadro di valore specifico per valutare e far fronte al danno. Infatti, bisogna notare come l'espressione "prodotto a duplice uso" non sia di facile definizione da un punto di vista concettuale e normativo. La letterature in materia si è spesso interrogata su quale sia la misura del danno al fine di considerare un determinato prodotto soggetto alla regolamentazione

32. Commissione europea, Raccomandazione (UE) 2024/2659 dell'11 ottobre 2024 relativa a orientamenti sull'esportazione di prodotti di sorveglianza informatica a norma dell'articolo 5 del regolamento (UE) 2021/821 del Parlamento europeo e del Consiglio, C/2024/7035, p.8.
33. Per una panoramica generale sull'impatto dell'intelligenza artificiale sui diritti umani, v. Quintavalla–Temperman 2023.
34. *Ibidem*.
35. *Ibidem*.

europea dei prodotti a duplice uso[36]. La risposta che viene convenzionalmente fornita è che un prodotto può essere considerato a duplice uso quando il suo uso (malevolo o negligente) ha un potenziale sufficiente per causare danni su larga scala a un insieme di valori che il legislatore ritiene opportuno proteggere legalmente. È proprio in questo contesto che il legislatore europeo ha scelto i diritti umani e il diritto internazionale umanitario come quadro di valore di riferimento.

Detto ciò, l'esito del processo legislativo ha evidenziato le sfide concrete che l'Unione europea incontra nell'integrare considerazioni in materia di diritti umani nelle sue relazioni commerciali esterne. La volontà della Commissione europea (e del Parlamento) di sviluppare un quadro più armonizzato ha dovuto rapportarsi con le esigenze di altre parti interessate. Per maggiore chiarezza, i singoli Stati membri – per mezzo del Consiglio quale istituzione coinvolta nel processo legislativo europeo – così come gli esportatori hanno insistito per una minore integrazione di considerazioni in materia di diritti umani.

Il quadro legislativo è dunque stato parzialmente limitato nella integrazione di considerazioni inerenti ai diritti umani. Tuttavia, il rischio di incertezza nella implementazione del regolamento è – almeno in parte – rimasto[37]. Gli Stati membri e finanche gli esportatori sono chiamati a valutare la sussistenza di gravi violazioni di diritti umani e diritto internazionale umanitario tramite quanto statuito dalle clausole onnicomprensive. In tal modo, si è potuto assistere a un trasferimento di una maggiore responsabilità volta a controllare la possibile sussistenza di rischi di violazione dei diritti umani dal livello europeo a quello nazionale. Questo trasferimento di responsabilità è sicuramente rispettoso di un principio di sussidiarietà solitamente molto caro agli Stati membri. Tuttavia, come notato dalla Commissione stessa nella sua proposta di modifiche al regolamento europeo nel 2016, sarebbe opportuno che l'Unione europea avesse una posizione comune circa la violazione dei diritti umani da parte di prodotti a duplice uso esportati al di fuori del territori europeo.

Dunque, il regolamento europeo sui prodotti a duplice uso si regge su un fragile bilanciamento tra la necessità di promuovere una politica commerciale comune secondo gli interessi degli attori economici e la integrazione di considerazioni in materia di diritti umani. L'articolo 3 esemplifica tale bilanciamento da un lato assicurando una lista a livello europeo di prodotti che necessitano di una autorizzazione all'esportazione e, dall'altro, ammettendo l'intervento da parte dei singoli Stati membri nel decidere quale prodotto possa violare i diritti umani. In quest'ottica, vi è il rischio che la caratterizzazione della valutazione dei diritti umani effettuata dagli Stati membri diventi un processo ancora più politico e discrezionale di quanto non sia già. Così facendo, una risposta nazionale potrebbe portare ad una maggiore frammentarietà del quadro normativo. Tale risultato sarebbe non solo disallineato con le richieste degli attori economici per un quadro normativo chiaro, ma porterebbe anche a non rafforzare la percezione di uno sviluppo dell'intelligenza artificiale come tecnologia affidabile a causa di una minore certezza del diritto all'interno dell'Unione europea.

Riferimenti bibliografici

Amnesty International (2020), *Out of Control: Failing EU Laws for Digital Surveillance Export*, Report, Amnesty International, 2020

BDI (2016), *EC Dual-Use: Review of the EC Dual-Use Regulation*, 2016

M. Bromley (2023), *The EU Dual-use Regulation, cyber-surveillance and human rights: the competing norms and organised hypocrisy of EU export controls*, in "Defence Studies", vol. 23, 2023, n. 4

DIGITALEUROPE (2018), *Updated DIGITALEUROPE Comments on Proposal for Recast of Export Control Regulation*, 2018

36. Per la discussione, v. Schmid–Riebe–Reuter 2022, p. 12.

37. Cfr. Di Franco 2022.

E. Di Franco (2022), *Assessing the role of human rights in the Recast EU Regulation on dual-use items*, Trans European Policy Studies Association Briefs, 2022

J. Donnelly (2013), *Universal human rights in theory and practice*, Cornell University Press, 2013

J. Donnelly (1982), *Human rights and human dignity: An analytic critique of non-Western conceptions of human rights*, in "American Political Science Review", vol. 76, 1982, n. 2

A. Fruscione (2022), *Dual Use Items: A Whole New Export Regulation in the European Union*, in "Global Trade and Customs Journal", vol. 17, 2022, n. 3

M.C. Horowitz (2019), *When speed kills: Lethal autonomous weapon systems, deterrence and stability*, in "Journal of Strategic Studies", vol. 42, 2019, n. 6

U. Jaremba, M. Kanetake, I. Koning (2019), *Economic and Non-Economic Values and Objectives in the EU's International Trade: Normative Tensions, Actors and Processes*, in "Europe and the World: A Law Review", vol. 3, 2019, n. 1

M. Kanetake (2020), *The EU's Dual-Use Export Control and Human Rights Risks: The Case of Cyber Surveillance Technology*, in "Europe and the World: A Law Review", vol. 3, 2019, n. 1

K.L. Meissner, K. Urbanski (2022), *Feeble Rules: One Dual-Use Sanctions Regime, Multiple Ways of Implementation and Application?*, in "European Security", vol. 31, 2022

A. Quintavalla, J. Temperman (2023), *Artificial intelligence and human rights*, Oxford University Press, 2023

L. Riecke (2023), *Unmasking the Term 'Dual Use' in EU Spyware Export Control*, in "European Journal of International Law", vol. 34, 2023, n. 3

S. Schmid, T. Riebe, C. Reuter (2022), *Dual-use and trustworthy? A mixed methods analysis of AI diffusion between civilian and defense R&D*, in "Science and engineering ethics", vol. 28, 2022, n. 2

D. Trusilo, D. Danks (2024), *Commercial AI, Conflict, and Moral Responsibility: A theoretical analysis and practical approach to the moral responsibilities associated with dual-use AI technology*, in "arXiv", 2402.01762, 2024

O.L. Van Daalen, J.V.J. Van Hoboken, M. Rucz (2023), *Export control of cybersurveillance items in the new dual-use regulation: The challenges of applying human rights logic to export control*, in "Computer Law & Security Review", vol. 48, 2023

RIVISTA ITALIANA
DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0237 • articolo sottoposto a peer review • pubblicato in anteprima il 25 set. 2025

Daniele Amoroso

La disciplina dei sistemi d'arma autonomi nel diritto internazionale umanitario. Stato dell'arte e prospettive di regolamentazione

Il presente contributo persegue un duplice obiettivo: da un lato, offrire una ricostruzione del quadro giuridico oggi applicabile ai sistemi d'arma autonomi, con specifico riferimento alle norme del diritto internazionale umanitario (DIU); dall'altro, tracciare le direttrici lungo le quali potrebbe svilupparsi una futura disciplina internazionale. Dopo aver chiarito la nozione di sistema d'arma autonomo, sono analizzate le norme del DIU attualmente applicabili, dedicando particolare attenzione alle revisioni giuridiche *ex* art. 36 del Primo Protocollo Addizionale. Si evidenzia come l'autonomia decisionale di tali sistemi imponga di verificarne non solo la liceità intrinseca, ma anche la capacità di rispettare i principi di distinzione e proporzionalità. Sono poi approfonditi gli obblighi derivanti dal principio di precauzione, in relazione alla progettazione dei sistemi e all'interazione uomo-macchina. Nella seconda parte si esaminano le principali proposte normative in discussione a livello internazionale, con un focus sull'approccio "two-tier" del CICR e sugli sviluppi negoziali più recenti, sia in seno al GGE sia presso l'Assemblea Generale dell'ONU.

Sistemi d'arma autonomi – Diritto internazionale umanitario – Articolo 36 del Primo Protocollo Addizionale alle Convenzioni di Ginevra – Principi di distinzione, proporzionalità e precauzione – Intelligenza artificiale

The Legality of Autonomous Weapons Systems under International Humanitarian Law: What the Law Says and How It Could Be Improved

This article pursues a twofold objective: on the one hand, it offers an overview of the legal framework currently applicable to autonomous weapons systems (AWS), with a focus on the rules of international humanitarian law (IHL); on the other hand, it outlines possible trajectories for the development of future international regulation on AWS. After clarifying the notion of AWS, the article examines the IHL norms applicable to their use, with particular emphasis on legal reviews under Article 36 of Additional Protocol I. It highlights how the decision-making autonomy of such systems requires not only an assessment of their intrinsic lawfulness but also of their capacity to comply with the principles of distinction and proportionality. The obligations stemming from the principle of precaution are also addressed, especially regarding the design of AWS and the human-machine interaction. The second part explores the main regulatory proposals currently on the table, zooming in on the ICRC's two-tier approach and the most recent developments within the GGE and the UN General Assembly.

Autonomous Weapons Systems – International Humanitarian Law – Article 36 of the First Additional Protocol to the Geneva Conventions – Principles of Distinction, Proportionality and Precaution – Artificial Intelligence

L'Autore è professore associato di Diritto internazionale, Università degli studi di Cagliari

Questo contributo fa parte della sezione monografica *Le due facce della rivoluzione digitale, tra emergenze e tecnologie* dual-use, a cura di Paolo Passaglia

1. Introduzione

È ormai ampiamente noto come i recenti sviluppi nel campo della robotica e dell'intelligenza artificiale (IA) abbiano reso possibile la progettazione di sistemi d'arma in grado di selezionare e colpire obbiettivi in modo autonomo, vale a dire senza che sia necessario un ulteriore intervento umano dopo l'attivazione. Sebbene il potenziale tecnologico di tali sistemi non sia ancora stato pienamente esplorato, esistono già oggi applicazioni operative concrete che rientrano a pieno titolo nella categoria dei sistemi d'arma autonomi.

Questa circostanza ha stimolato una produzione scientifica vastissima e multidisciplinare, rendendo il tema uno degli ambiti più affollati del dibattito contemporaneo tra studiosi di diritto internazionale, etica applicata e teoria delle relazioni internazionali[1]. La riflessione sull'accettabilità etico-giuridica di questi sistemi, e ancor più sulla loro disciplina, ha rapidamente travalicato i confini accademici, diventando oggetto di una vivace e persistente discussione politica e diplomatica.

Un ruolo determinante in questa evoluzione è stato giocato dalla società civile organizzata: la mobilitazione, a partire dal 2013, della Campagna internazionale per la messa al bando dei sistemi d'arma autonomi (*Campaign to Stop Killer Robots*, SKR) ha contribuito in modo decisivo a porre la questione all'ordine del giorno dei principali fora multilaterali[2]. In particolare, le implicazioni normative dell'autonomia dei sistemi d'arma sono da quasi un decennio al centro dei lavori di un Gruppo di esperti governativi (GGE) istituito nel quadro della Convenzione su certe armi convenzionali (CCW), e più recentemente sono approdate anche in seno all'Assemblea Generale delle Nazioni Unite.

Ripercorrere per intero questo dibattito, nelle sue articolazioni tecniche, normative e politiche,

1. Si considerino, per limitarci ai lavori monografici che affrontano la questione nella prospettiva del diritto internazionale: Copeland 2025, Valdares Fernandes Barbosa 2025, Kwik 2024, de Vries 2023, Bode–Huells 2022, Mauri 2022, Seixas-Nunes 2022, Saxon 2021, Amoroso 2020, McFarland 2020.
2. Carpenter 2014, p. 88 ss. V. anche, per ulteriori informazioni, il sito della Campagna.

risulterebbe non solo impossibile nello spazio assegnato, ma anche superfluo, vista la già estesa letteratura esistente. Il presente lavoro si propone dunque un obiettivo più circoscritto: per un verso, offrire una ricostruzione ragionata del quadro giuridico oggi applicabile ai sistemi d'arma autonomi, con particolare riferimento alle norme del diritto internazionale umanitario (o diritto internazionale dei conflitti armati), che per ragioni evidenti ne costituiscono l'ambito regolamentare d'elezione; per altro verso, tracciare alcune direttrici lungo le quali potrebbe svilupparsi, o consolidarsi, una futura disciplina internazionale, esplorandone l'effettiva praticabilità anche in considerazione delle tensioni che, allo stato attuale, dividono la comunità internazionale.

Dopo aver chiarito, nel par. 2, la nozione di sistema d'arma autonomo e le principali tipologie oggi esistenti o in via di sviluppo, verranno analizzate, nei parr. 3 e 4, le norme del DIU che concorrono a definire la disciplina attualmente applicabile ai sistemi d'arma autonomi. Il par. 3, in particolare, si concentrerà sul ruolo delle revisioni giuridiche dei mezzi di combattimento ex art. 36 del Primo Protocollo Addizionale, evidenziando come l'autonomia decisionale di questi sistemi crei una sfida concettuale inedita, in quanto impone di verificare non solo la liceità intrinseca dell'arma, ma anche la sua capacità concreta di operare nel rispetto dei principi che regolano il *targeting*, *in primis* quelli di distinzione e proporzionalità. Il par. 4 approfondirà, invece, gli obblighi derivanti dal principio di precauzione e le implicazioni di tale principio in relazione alla progettazione dei sistemi e all'interazione tra macchina e operatore umano. Il par. 5 proporrà una sintesi degli obblighi che si possono ricavare dal quadro normativo esistente, soffermandosi in particolare sulle condizioni che consentono, o meno, l'impiego lecito di sistemi d'arma autonomi. Le prospettive di regolamentazione *de lege ferenda* saranno invece affrontate nel par. 6, che illustrerà le principali proposte attualmente in discussione a livello internazionale, con particolare attenzione all'approccio "two-tier" del Comitato internazionale della Croce Rossa (par. 6.1) e ai più recenti sviluppi negoziali sia in seno al GGE sia in ambito ONU (par. 6.2). Il par. 7 conclude con alcune osservazioni sul futuro della regolazione multilaterale in materia.

2. Definizione operativa e tipologie di sistemi d'arma autonomi

Un sistema d'arma autonomo può essere definito come un sistema in grado di selezionare e colpire un obbiettivo senza che, dopo la sua attivazione, sia necessario un ulteriore intervento umano. Pur non essendo esente da criticità, in particolare per la sua eccessiva inclusività, questa definizione rappresenta un punto di partenza difficilmente eludibile nella discussione, essendo condivisa da una pluralità di attori istituzionali e non governativi coinvolti nel dibattito[3]. Essa è infatti riprodotta – con variazioni marginali – in documenti e dichiarazioni ufficiali, non solo della Campagna per la messa al bando delle armi autonome[4], ma anche di soggetti portatori di istanze in tutto o in parte divergenti, come il Dipartimento della Difesa degli Stati Uniti[5] e il Comitato internazionale della Croce Rossa[6].

È importante sottolineare che il ricorso a sistemi di intelligenza artificiale non costituisce un elemento necessario di questa definizione. L'IA non è, cioè, una componente costitutiva dei sistemi d'arma autonomi, bensì un "abilitatore tecnologico" (*enabler*) della loro autonomia operativa, in particolare nei sistemi più sofisticati e adattivi[7]. In tal senso, la distinzione tra armi autonome "con" o "senza" IA può avere rilevanza funzionale, ma non incide sulla qualificazione giuridica di un sistema come autonomo.

La definizione operativa appena richiamata, come si è detto, è particolarmente ampia. Alcuni sistemi che vi rientrano a pieno titolo sono già oggi in uso, seppure in contesti circoscritti e con finalità

3. Per un tentativo di definizione più raffinato e scientificamente accurato, v. Taddeo-Blanchard 2022.
4. Human Rights Watch 2012.
5. Department of Defense, Directive 3000.09, *Autonomy in Weapons Systems (2012)*, riformata nel 2023.
6. Comitato internazionale della Croce Rossa 2021.
7. Asaro 2019, p. 60.

prevalentemente difensive[8]. È il caso, ad esempio, dei sistemi di difesa aerea come l'*Iron Dome* israeliano, progettati per reagire in modo automatico a minacce in arrivo,[9] o delle tipologie più avanzate di munizioni "fire and forget", come il *Brimstone* britannico.[10] Un altro esempio frequentemente citato è quello dei robot sentinella sudcoreani SGR-A1 e Super aEgis II[11]: pur essendo tecnicamente in grado di identificare e colpire autonomamente un obbiettivo, per quanto è dato sapere questi sistemi vengono attualmente impiegati in modalità semi-autonoma, nella quale l'individuazione dell'obbiettivo viene effettuata dalla macchina, ma la decisione di aprire il fuoco resta affidata a un operatore umano.[12] Particolarmente rilevanti sono poi le cosiddette munizioni circuitanti (*loitering munitions*), come l'Harpy NG israeliano, un drone-suicida capace di pattugliare un'area per diverse ore alla ricerca di sorgenti di onde radio su cui abbattersi, senza che l'operatore umano debba intervenire oltre l'attivazione iniziale[13].

Altri sistemi, attualmente in fase di sperimentazione, sembrano destinati a potenziare ulteriormente l'autonomia decisionale in ambito operativo. Si pensi ai prototipi di caccia autonomi controllati da IA, capaci di ingaggiare vittoriosamente duelli aerei con piloti esperti[14]; o alle ricerche nel campo della *swarm robotics*, che stanno aprendo la strada allo sviluppo dei cd. "sciami" di droni armati, di piccole dimensioni e a basso costo, il cui spiegamento in numero massivo – nell'ordine delle centinaia, se non delle migliaia – dovrebbe consentire di sopraffare le difese aeree nemiche attraverso attacchi di saturazione improvvisi e coordinati[15].

3. La *lex lata*: l'art. 36 del Primo Protocollo Addizionale alle Convenzioni di Ginevra

L'analisi delle norme internazionali applicabili ai sistemi d'arma autonomi, in quanto tecnologie emergenti, non può che prendere le mosse dall'art. 36 del Primo Protocollo Addizionale alle Convenzioni di Ginevra del 1977. Questa disposizione, significativamente rubricata "Nuove armi", sancisce infatti l'obbligo per le Parti Contraenti di stabilire, "[i]n caso di studio, sviluppo, acquisizione o adozione di una nuova arma", se il suo impiego sia, "in determinate o in tutte le circostanze, vietato dal […] Protocollo o da qualsiasi altra norma di diritto internazionale applicabile".

In quanto disposizione pattizia, l'art. 36 vincola solo gli Stati che hanno ratificato il Primo Protocollo. Va tuttavia rilevato che, tra la manciata di Stati che non sono parte del Protocollo, alcuni tra i più rilevanti dal punto di vista militare – come gli Stati Uniti[16] e Israele[17] – conducono comunque regolarmente revisioni giuridiche dei nuovi mezzi di combattimento[18]. La rilevanza dell'obbligo in questione per i sistemi d'arma autonomi, del resto, è stata espressamente riconosciuta nei Principi Guida adottati per *consensus* dal GGE sui sistemi d'arma autonomi letali, che incorporano – quasi *ad litteram* – il testo dell'art. 36[19].

Si tratta, all'evidenza, di un obbligo procedurale, volto a garantire che l'introduzione di nuove tecnologie belliche nell'arsenale statale avvenga nel rispetto del diritto internazionale vigente. Tradizionalmente, tale revisione giuridica mira ad accertare la conformità del nuovo sistema con le norme

8. Boulanin–Verbruggen 2017.
9. *Ivi*, p. 36 ss.
10. *Ivi*, p. 47 ss.
11. *Ivi*, p. 44 ss.
12. Parkin 2015.
13. Boulanin–Verbruggen 2017, p. 50 ss.
14. Losey 2024.
15. Ekelhof–Persi Paoli 2020.
16. *Army regulation 27-53* (1979), riformata da ultimo nel 2019.
17. Jevglevskaja 2018, p. 209.
18. Tale circostanza ha suggerito che l'obbligo in questione abbia in realtà natura consuetudinaria (Jevglevskaja 2018).
19. *Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems*, 25 settembre 2019, CCW/GGE.1/2019/3, Annex IV, Guiding Principles, Principle (e).

del diritto internazionale umanitario che vietano o disciplinano l'uso di determinate categorie di armi – si pensi, ad esempio, alla messa al bando dei laser accecanti o al divieto delle armi che causano mali superflui o sofferenze inutili. Nel caso dei sistemi d'arma autonomi, tuttavia, la situazione risulta concettualmente più complessa. Come osservato dalla delegazione svizzera nei dibattiti che hanno preceduto l'istituzione del GGE, tali sistemi sono concepiti per portare a termine l'intero ciclo di *targeting* senza intervento umano[20]. Ciò comporta un ampliamento dell'ambito della revisione giuridica: non è sufficiente interrogarsi sulla liceità dell'arma in sé, ma occorre valutare se, e in quali condizioni, essa sia in grado di operare nel rispetto delle norme che regolano il *targeting* secondo il diritto internazionale umanitario[21].

Ne deriva, pertanto, un arricchimento sostanziale dei criteri da considerare nella revisione giuridica. In particolare, occorre valutare se il sistema sia, in concreto, capace di operare nel rispetto dei principi fondamentali del diritto dei conflitti armati: il principio di distinzione e il principio di proporzionalità[22]. Il terzo cardine del diritto del *targeting* – il principio di precauzione – sarà invece esaminato più avanti, in quanto pone questioni che meritano un approfondimento separato.

Prima di soffermarsi sui problemi specifici posti dall'autonomia dei sistemi d'arma rispetto ai principi appena citati, occorre richiamare un ulteriore aspetto rilevante degli obblighi di revisione giuridica. Tanto l'art. 36 quanto i Principi Guida chiariscono che un nuovo mezzo di combattimento (e, dunque, un sistema d'arma autonomo) può essere vietato "*in alcune* o in tutte le circostanze". Tale formulazione consente una valutazione graduata, che non si esaurisce nell'analisi delle caratteristiche intrinseche del sistema, ma considera anche le condizioni concrete del suo impiego. Ne consegue che l'impiego di un sistema d'arma autonomo può essere ritenuto lecito in presenza di determinate condizioni, pur risultando inammissibile in altre.

3.1. Il principio di distinzione

Il principio di distinzione rappresenta uno dei cardini del diritto internazionale umanitario e impone alle parti in conflitto l'obbligo di distinguere, in ogni circostanza, tra civili e combattenti, nonché tra beni civili e obbiettivi militari. L'art. 48 del Primo Protocollo Addizionale alle Convenzioni di Ginevra del 1977 stabilisce la regola generale secondo cui "le Parti in conflitto devono in ogni momento distinguere tra popolazione civile e combattenti, nonché tra beni civili e obiettivi militari, e dirigere le loro operazioni soltanto contro obiettivi militari". Questa disposizione è ripresa e specificata negli articoli 51(2) e 52(1) del medesimo Protocollo, che disciplinano rispettivamente la protezione della popolazione civile e dei beni civili.

A queste norme si affiancano altre disposizioni che, pur non essendo volte alla protezione dei civili, pongono analoghi problemi di distinzione, come il divieto di attaccare persone *hors de combat* (art. 41(2) Primo Protocollo), ovvero i combattenti della parte avversa che hanno manifestato l'intenzione di arrendersi o si trovano in stato di incapacità a causa di ferite, naufragio o malattia, a condizione che si astengano da atti ostili e non tentino la fuga[23].

Il contenuto normativo del principio, almeno nella sua formulazione astratta, appare chiaro. Tuttavia, la sua applicazione concreta è resa complessa dal persistere di zone grigie, in particolare nel contesto degli scenari operativi urbani. In queste situazioni, i combattenti si confondono con la popolazione civile ed i beni civili sono spesso impiegati a fini militari. Si considerino, in particolare, la partecipazione diretta alle ostilità da parte di civili (art. 51(3) del Protocollo), che determina la sospensione temporanea della loro protezione o la qualificazione degli oggetti cd. *dual use* come obbiettivi militari legittimi, in virtù della loro destinazione o impiego effettivo, secondo la definizione contenuta nell'art. 52(2) del Protocollo.

20. Svizzera, *Towards a "compliance-based" approach to LAWS*, CCW Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), Ginevra, 30 marzo 2016.
21. Copeland 2025, p. 152.
22. *Ivi*, p. 245.
23. Per una disamina più ampia delle altre norme del DIU che pongono problemi di distinzione v. Amoroso 2020, p. 56 ss.

Questa complessità si riverbera inevitabilmente sulla capacità dei sistemi d'arma autonomi di rispettare il principio di distinzione. Non vi è dubbio, infatti, che alcuni compiti di identificazione presupposti dal principio di distinzione possano essere eseguiti, con un livello di affidabilità accettabile, sulla base delle tecnologie esistenti. Questo è senz'altro il caso del riconoscimento di oggetti "cooperativi" – ossia quelli che emettono segnali rilevabili, come radar o transponder: l'Harpy NG israeliano, per fare un esempio relativamente noto, è in grado di identificare gli obbiettivi su cui farsi esplodere sulla sola base delle onde radio da questi emesse.[24] Lo stesso vale per il riconoscimento degli oggetti che sono obbiettivi militari *per natura*, come carri armati, elicotteri o missili. Sia i sistemi di difesa aerea, sia le munizioni "fire and forget" più sofisticate (come il *Brimstone* britannico) sono in grado di identificare autonomamente questa tipologia di obbiettivi.[25]

Va detto, peraltro, che diverse norme del DIU mirano proprio a facilitare l'identificazione degli obbiettivi legittimi nonché di persone e oggetti protetti. Alcune norme, in particolare, promuovono la "cooperazione" degli oggetti protetti affinché non vengano colpiti erroneamente. L'Allegato I del Primo Protocollo, ad esempio, contiene disposizioni molto dettagliate che regolano l'emissione di specifici segnali luminosi, radio ed elettronici da parte di aeromobili, navi e veicoli medici, al fine di renderli facilmente individuabili dalle Parti in conflitto.[26] Altre norme, invece, richiedono l'esibizione di segni distintivi facilmente distinguibili per segnalare che un certo oggetto è protetto dal DIU. Si pensi, a questo proposito, alle disposizioni che regolano l'uso dell'emblema della Croce Rossa (e simili) per il servizio medico, dello Scudo blu per i beni culturali e dei tre cerchi arancioni che segnalano "opere e installazioni contenenti forze pericolose"[27]. Lo stesso vale per l'obbligo dei combattenti "di distinguersi dalla popolazione civile [ad es. indossando uniformi] mentre sono impegnati in un attacco o in un'operazione militare in preparazione di un attacco"[28]. Questi obblighi, pur essendo originariamente concepiti per facilitare l'applicazione del principio di distinzione da parte dei combattenti umani, finiscono per semplificare i compiti percettivi assegnati ai sistemi d'arma autonomi, che dovranno essere progettati in modo da essere in grado di riconoscere i segnali (luminosi o di altro tipo) provenienti da oggetti protetti o di identificare i segni distintivi.

Anche alcuni compiti più complessi, ma comunque assistiti da marcatori visivi o comportamentali, possono teoricamente essere affrontati da sistemi autonomi. Si pensi all'identificazione di un combattente che manifesta l'intenzione di arrendersi, a condizione che tale gesto sia chiaramente codificato (ad es., le mani alzate). Secondo alcuni report, la sentinella robotica SGR-A1 sarebbe capace di riconoscere segnali di resa[29]. Va tuttavia sottolineato, però, che tale sistema opera in un contesto, la zona demilitarizzata tra le due Coree, caratterizzato dalla sostanziale assenza di elementi che possano disturbare il riconoscimento autonomo.

Molto più problematici sono, invece, i compiti che implicano valutazioni contestuali e interpretazioni dinamiche. Si pensi al riconoscimento di civili che partecipano direttamente alle ostilità, alla qualificazione di un oggetto come obbiettivo militare per uso o scopo (ad esempio, una scuola adibita a deposito di munizioni) o, più in generale, all'applicazione del principio di distinzione in scenari di guerriglia urbana, caratterizzati dalla compresenza di obiettivi legittimi e persone/beni protetti. In questi casi, il rispetto del principio di distinzione presuppone non solo la percezione degli elementi fisici dell'ambiente, ma anche la comprensione della loro funzione, del contesto operativo e dell'evoluzione della situazione – competenze che, allo

24. Scharre 2018, p. 84.

25. Boulanin–Verbruggen 2017, rispettivamente pp. 37-39 e 49-50.

26. Artt. 6-8, 10-11.

27. V., rispettivamente, art. 44 della Prima Convenzione di Ginevra del 1949, artt. 16-17 della Convenzione dell'Aja del 1954 sulla protezione dei beni culturali nei conflitti armati e art. 56, co. 7, del Primo Protocollo.

28. Art. 44, co. 3, del Primo Protocollo.

29. Boulanin–Verbruggen 2017, p. 45.

stato attuale, sono ancora al di fuori della portata dell'IA[30].

Tutto ciò non esclude che sviluppi tecnologici futuri possano estendere la capacità valutativa dei sistemi autonomi a scenari oggi considerati fuori portata. L'impiego di architetture basate su *deep learning* e l'addestramento su dataset estesi e realistici potranno consentire una sofisticazione percettiva e inferenziale sempre maggiore. Tuttavia, il salto qualitativo richiesto per colmare il divario tra cognizione algoritmica e giudizio umano in questi contesti operativi resta notevole, e al momento non vi sono evidenze concrete che tale traguardo sia prossimo.

3.2. Il principio di proporzionalità

Il principio di proporzionalità, codificato all'art. 51(5)(b) e ribadito all'art. 57(2)(a)(iii) del Primo Protocollo Addizionale, vieta quegli attacchi che ci si attende provochino incidentalmente danni ai civili o a beni civili (c.d. danni collaterali) eccessivi rispetto al vantaggio militare concreto e diretto previsto. Un attacco, pertanto, non diventa illecito per il semplice fatto di causare danni collaterali. Piuttosto, in base al principio di proporzionalità, la sua legittimità è subordinata ad una valutazione *ex ante*, fondata su tre passaggi logici:

- la stima del danno collaterale previsto (in vite umane e beni civili);
- la valutazione del vantaggio militare atteso;
- la determinazione dell'eccessività del primo rispetto al secondo.

Di questi tre passaggi, l'unico che si presta agevolmente ad essere gestito da sistemi autonomi è la stima del danno collaterale. Le forze armate, a partire da quelle statunitensi, fanno già ampio uso di sistemi software per stimare, in sede di pianificazione, l'impatto di un attacco su persone, edifici e infrastrutture civili[31]. Questi strumenti permettono infatti di calcolare, con un certo grado di affidabilità, la portata dell'esplosione, la propagazione delle schegge, il danno strutturale indotto su edifici contigui e il rischio per persone presenti in aree adiacenti.

Più complessa è la valutazione del vantaggio militare. A differenza di quanto avviene per il principio di distinzione, non è sufficiente stabilire che un determinato bene o una persona costituisce un obbiettivo legittimo perché la sua eliminazione o distruzione offre "un vantaggio militare concreto". Chi decide l'attacco, infatti, dovrà attribuire un valore al vantaggio militare in questione, al fine di confrontarlo con i danni stimati[32]. Qui entrano in gioco fattori non sempre facili da quantificare e soggetti a variazione nel tempo e nello spazio: tra gli altri, l'importanza tattica o strategica del *target*, la fase del conflitto, o il grado di certezza circa il successo dell'azione.

Il passaggio più resistente ad una codificazione algoritmica è però rappresentato dal cuore del principio di proporzionalità: la valutazione dell'eccessività dal danno collaterale. Tale giudizio implica infatti un bilanciamento tra valori disomogenei, come il numero di civili potenzialmente colpiti e l'importanza tattica di un'infrastruttura militare[33]. Di conseguenza, il principio di proporzionalità non si presta ad un'applicazione "binaria", come avviene per il principio di distinzione, per cui – nonostante le difficoltà che abbiamo visto sopra – è almeno astrattamente possibile stabilire se un bene o una persona siano protetti o meno dal DIU[34].

Lo standard elaborato nella prassi per orientare l'applicazione del principio di proporzionalità, quello del "comandante militare ragionevole"[35], si limita invero a definire una zona di ragionevole discrezionalità, che ricomprende una pluralità di decisioni sulla proporzionalità – alcune più attente alla protezione dei civili, altre più orientate alla massimizzazione del vantaggio militare – tutte considerate legittime[36].

30. Human Rights Watch 2025, p. 19; Comitato internazionale della Croce Rossa 2024, p. 65.
31. Thurnher 2014, p. 222.
32. Holland 2004, p. 54.
33. Fenrick 1982, p. 94.
34. Cannizzaro 2014, p. 332.
35. Sul quale v., anche per ulteriori riferimenti, Henderson–Reece 2018, p. 845.
36. In questo senso, v. Corte suprema israeliana, *Beit Sourik Village Council v. The Government of Israel*, HCJ 2056/04, 30 maggio 2004, parr. 42 e 46. La scelta tra queste opzioni, anche se libera da vincoli giuridici, è evidentemente gravida di conseguenze e implicazioni morali (Kennedy 2004, pp. 290-291).

La difficoltà di tradurre in un codice di programmazione uno standard tanto vago nei suoi contenuti applicativi è evidente. Non deve dunque sorprendere che anche autori favorevoli a un impiego robusto dei sistemi d'arma autonomi siano disposti ad ammettere che la valutazione dell'eccessività debba rimanere affidata al decisore umano, che la effettuerebbe in fase di pianificazione dell'attacco[37].

4. Sempre sulla *lex lata*: il principio di precauzione

Oltre all'art. 36 del Primo Protocollo Addizionale, un'altra norma fondamentale di riferimento, ancora in una prospettiva *de lege lata*, è rappresentata dal principio di precauzione, che impone alle Parti in conflitto di adottare tutte le misure *praticabili* per garantire il rispetto dei principi di distinzione e proporzionalità.

Il principio, codificato all'art. 57 del Primo Protocollo, si traduce essenzialmente in una serie di obblighi positivi, volti a prevenire violazioni del diritto umanitario. Tra questi, rilevano in particolare:

- l'obbligo di fare tutto il possibile per assicurare la corretta identificazione del target come obiettivo militare[38];
- l'obbligo di fare tutto il possibile per mantenere il controllo sull'esecuzione dell'attacco, così da poterlo annullare o sospendere quando ciò sia necessario per evitare un attacco diretto contro la popolazione civile o danni collaterali eccessivi[39].

Ciò ha importanti implicazioni per un modello normativo di relazione tra operatori umani e sistemi d'arma. Anzitutto, come si è visto, il principio di precauzione obbliga le Parti in conflitto a mobilitare tutti i mezzi a loro disposizione, ove ragionevolmente disponibili, per facilitare la corretta qualificazione del *target* come obbiettivo legittimo[40]. Se, dunque, il coinvolgimento di operatori umani è idoneo a favorire una maggiore precisione negli attacchi, la loro inclusione nel processo decisionale deve considerarsi obbligatoria in virtù del principio di precauzione. A questo fine, i sistemi devono essere progettati in modo da consentire ad operatori adeguatamente formati di controllarne e limitarne gli effetti.

Il principio di precauzione sollecita quindi una riflessione sul modo in cui le macchine prendono decisioni e, soprattutto, su come possono sbagliare. Anche i sistemi di IA più avanzati, infatti, continuano ad essere soggetti a errori imprevedibili e controintuitivi, talvolta difficilmente comprensibili perfino da coloro che li hanno programmati e istruiti[41]. Si tratta di errori diversi da quelli umani, che non derivano da stanchezza o stress, ma da fallimenti percettivi o cognitivi legati al cosiddetto "gap semantico": l'IA non comprende il significato delle informazioni che elabora, ma effettua correlazioni tra moli enormi di dati a velocità sovrumana[42].

Questo rende l'IA vulnerabile a distorsioni di contesto, illusioni percettive o manipolazioni intenzionali (*adversarial attacks*)[43] – vulnerabilità cui l'operatore umano è in larga misura immune. Se si considera che, nel contesto di un conflitto armato, questi errori possono tradursi in attacchi diretti contro la popolazione civile (o comunque in gravi danni collaterali), appare evidente quanto sia poco sensato affidare il ciclo di *targeting* interamente alla macchina, così come sarebbe irragionevole escluderla *a priori*. Il principio di precauzione richiede invece un modello di interazione sinergica tra operatore umano e sistema, in cui ciascuno compensi i limiti dell'altro[44]. Naturalmente, ciò

37. V., tra gli altri, Zajac 2023; Henderson–Keane–Liddy 2017, p. 352, Schmitt–Thurnher 2013, p. 256.
38. Sul punto, si veda la preziosa codificazione del DIU consuetudinario pubblicata dal CICR (Henckaerts–Doswald-Beck 2005, Regola 16).
39. *Ivi*, Regola 19.
40. Mancini 2006, p. 278.
41. Liu–Wei–Liu–Davis 2025.
42. Comitato internazionale della Croce Rossa 2019, p. 20.
43. Si noti che tali manipolazioni delle immagini sono spesso impercettibili (o comunque irrilevanti) per un essere umano (Chowdhury 2025).
44. Sharkey 2016, p. 23 ss.

non implica un coinvolgimento umano irrealistico: in alcuni contesti, come quello dei sistemi di difesa antimissile (ad esempio, *Iron Dome*), la previsione di un controllo umano accurato sulle singole decisioni di *targeting* comporterebbe rischi inaccettabili per la sicurezza delle persone. Ma proprio perché gli obblighi derivanti dal principio di precauzione sono condizionati alla praticabilità (*feasibility*), il diritto internazionale non esige l'impossibile.

5. Conclusioni *de lege lata*

Dall'analisi fin qui svolta emerge con sufficiente chiarezza che il diritto internazionale umanitario, pur non contenendo norme esplicitamente dedicate ai sistemi d'arma autonomi, dispone già di strumenti adeguati a valutarne la liceità. L'art. 36 del Primo Protocollo Addizionale, come si è detto, rappresenta il primo snodo obbligato: in quanto clausola di verifica preventiva, esso impone agli Stati di stabilire se l'introduzione di un nuovo sistema d'arma sia compatibile con le norme esistenti del diritto internazionale, *in alcune o in tutte le circostanze*. Con riferimento ai sistemi d'arma autonomi, ciò presuppone una verifica della capacità di questi sistemi di svolgere il ciclo di *targeting* nel rispetto dei principi di distinzione e proporzionalità. La conclusione cui si è giunti, sulla base delle tecnologie esistenti e note, è che l'impiego di sistemi d'arma autonomi supera il test di legalità di cui all'art. 36 soltanto in presenza di alcune condizioni.

Nei contesti operativi più problematici – in particolare, in scenari urbani caratterizzati dalla prossimità fisica tra obiettivi legittimi e beni protetti – il loro utilizzo richiede infatti estrema cautela. In tali situazioni, la conformità ai principi di distinzione e proporzionalità presuppone valutazioni complesse e contestuali, che allo stato attuale solo un operatore umano può svolgere in modo attendibile. Di conseguenza, la legalità dell'impiego di sistemi autonomi in questi contesti può essere garantita solo a condizione che le decisioni critiche siano assunte in fase di pianificazione, sotto la responsabilità di un comandante umano.

Il ricorso a forme di *targeting* dinamico (vale a dire, non pianificato) da parte del sistema d'arma può essere ipotizzato, in linea di principio, solo in contesti operativi molto specifici, come ambienti desertici o marittimi, in cui:

- l'assenza di civili sia ragionevolmente certa, oppure
- i civili siano chiaramente separati, in termini spaziali o temporali, dagli obiettivi militari da colpire.

In ogni caso, indipendentemente dallo scenario operativo, il diritto internazionale umanitario richiede, in virtù del principio di precauzione, che sia mantenuta una forma di supervisione umana, almeno come *fail-safe*, cioè come meccanismo di sicurezza capace di bloccare o interrompere l'azione del sistema per evitare danni a persone e beni civili[45].

Affinché il coinvolgimento umano possa svolgere effettivamente questo ruolo, tuttavia, è necessario rispettare due ulteriori requisiti. Da un lato, la formazione degli operatori deve mirare a preservarne il senso critico, ponendo l'accento non solo sulle capacità ma anche sui limiti della macchina, al fine di evitare che soccombano al cd. *bias* dell'automazione. Dall'altro, i sistemi devono essere progettati con un'interfaccia che privilegi la trasparenza e la spiegabilità delle decisioni, così da rendere effettiva l'interazione uomo-macchina anche in condizioni di elevato stress operativo[46].

6. Prospettive *de lege ferenda*: verso uno strumento giuridicamente vincolante?

La disciplina dei sistemi d'arma autonomi resta dunque affidata, per il momento, all'interpretazione di norme generali del diritto internazionale umanitario, in particolare l'art. 36 del Primo Protocollo Addizionale e i principi che governano i processi di *targeting* (distinzione, proporzionalità e precauzione). Nonostante l'assenza di uno strumento giuridico dedicato, da queste norme è possibile ricavare, seppure con qualche sforzo esegetico, una serie di obblighi specifici relativi all'impiego di tali tecnologie che sembrano delineare un quadro regolatorio coerente e, tutto sommato, soddisfacente. Viene

45. Scharre 2016, p. 154. La compatibilità tra autonomia operativa e supervisione umana è stata, del resto, espressamente riconosciuta nella Direttiva 3000.09 del Dipartimento della Difesa, che include nella nozione di sistemi d'arma autonomi i sistemi "autonomi con supervisione dell'operatore" (*operator-supervised autonomous weapons systems*). V. Direttiva 3000.09, cit., p. 21.

46. Su questi aspetti, v. Amoroso 2020, p. 246 ss.

allora da interrogarsi sulle ragioni – e i meriti – dell'insistenza, da parte della società civile e di un numero sempre crescente di Stati, sulla necessità di adottare uno strumento giuridico *ad hoc*, sia esso un protocollo aggiuntivo alla CCW o un trattato autonomo. Un'insistenza che ha trovato una significativa eco istituzionale nei ripetuti appelli del Segretario Generale delle Nazioni Unite a concludere entro il 2026 i negoziati su uno strumento normativo in materia[47].

A parere di chi scrive, vi sono almeno tre considerazioni che concorrono a giustificare l'adozione di un nuovo strumento giuridico vincolante.

In primo luogo, uno strumento *ad hoc* potrebbe rendere espliciti e operativamente chiari quegli obblighi che oggi possono essere solo ricavati in via interpretativa. Chi impiega un sistema d'arma autonomo, come qualsiasi militare, ha bisogno di regole che siano immediatamente applicabili senza dover ricorrere a complesse mediazioni ermeneutiche. Un nuovo trattato, inoltre, potrebbe introdurre regole non desumibili dalle norme esistenti, ma fondate su istanze etiche condivise a livello internazionale. È in questo spazio che si colloca la proposta di vietare lo sviluppo e l'impiego di sistemi d'arma autonomi "anti-persona". Tale proposta poggia, infatti, su preoccupazioni legate al rispetto della dignità umana e al ruolo insostituibile della coscienza morale nell'uso della forza letale[48]. Infine, un trattato dedicato permetterebbe di creare un quadro istituzionale stabile, in grado di garantire non solo l'adozione di regole condivise, ma anche la loro attuazione effettiva attraverso meccanismi di monitoraggio, trasparenza, revisione tra pari e *confidence-building*.

6.1. L'approccio "two-tier" proposto dal Comitato internazionale della Croce Rossa

Nel 2021, all'esito di una lunga riflessione, il Comitato internazionale della Croce Rossa (CICR) ha pubblicato un *position paper* con una proposta di regolamentazione dei sistemi d'arma autonomi che, per la chiarezza della formula e l'autorevolezza della fonte, ha fortemente influenzato il dibattito successivo[49]. L'approccio promosso dal CICR si articola su due livelli (*two-tier approach*): da un lato, il divieto assoluto di sistemi d'arma autonomi "anti-persona" (ovvero: progettati per identificare e colpire esseri umani) e di quelli intrinsecamente imprevedibili; dall'altro, una serie di restrizioni operative volte a garantire un controllo umano contestualmente adeguato sui sistemi d'arma autonomi non coperti dai divieti.

Le restrizioni proposte dal CICR includono: limiti alla tipologia di *target* che possono essere ingaggiati autonomamente (in particolare, soltanto oggetti che costituiscono obiettivi militari *per natura*); limiti alla durata, all'ampiezza geografica e all'entità del loro impiego; limiti relativi al contesto operativo, con la previsione dell'utilizzo di tali sistemi soltanto in teatri caratterizzati dall'assenza di civili o comunque da una netta separazione tra questi e gli obbiettivi legittimi. Inoltre, i sistemi – pur essendo autonomi – dovranno essere sempre soggetti alla supervisione di un operatore umano, che avrà la possibilità di interrompere il funzionamento dell'arma esercitando il veto sulle decisioni di *targeting*.

È interessante notare come la proposta del CICR non utilizzi espressamente la nozione di "controllo umano significativo", che pure aveva orientato (e ancora in parte orienta) la discussione su questo tema[50]. Se questo è vero, è altresì vero che l'approccio *two-tier* è ampiamente compatibile con tale nozione, potendone anzi costituire un'articolazione concreta. Vale la pena osservare, inoltre, che i limiti operativi indicati dal Comitato riflettono e specificano gli obblighi che abbiamo ricavato a partire dall'art. 36 del Primo Protocollo e dal principio di precauzione. L'innovazione più rilevante della proposta del CICR è rappresentata

47. V., da ultimo, *'Politically unacceptable, morally repugnant': UN chief calls for global ban on 'killer robots'*, 14 May 2025, UN News.

48. Su questi aspetti, v. Mauri 2022, Saxon 2021.

49. Comitato internazionale della Croce Rossa 2021.

50. La nozione di controllo umano significativo era stata originariamente introdotta nel dibattito dall'ONG Article36 (Article36 2013). Più di recente, ad essa si è fatto riferimento anche in ambiti diversi da quello militare (ad esempio, veicoli autonomi, robot chirurgici, etc.). Su questo, v. Mecacci–Amoroso–Cavalcante Siebert et al. 2024.

infatti dal divieto generalizzato dei sistemi d'arma autonomi anti-persona, giustificato – come si è detto – da considerazioni etiche, legate alla tutela della dignità umana e all'impossibilità di delegare ad un agente artificiale il potere di decidere della vita e della morte di un essere umano.

6.2. Da Ginevra a New York (e ritorno): il progressivo coinvolgimento dell'Assemblea Generale e il *rolling text*

Grazie ad una tenace attività di lobbying da parte della società civile, negli ultimi anni il dibattito diplomatico sui sistemi d'arma autonomi è progressivamente uscito dai confini del GGE di Ginevra, per trovare spazio anche nel più inclusivo foro dell'Assemblea Generale delle Nazioni Unite. Anche se la discussione a New York non ha ancora prodotto sviluppi di rilievo, molto preziosa si è rivelata l'iniziativa, decisa con la Risoluzione 78/241, di affidare al Segretario Generale il compito di raccogliere e sintetizzare le posizioni degli Stati sulla regolamentazione dei sistemi d'arma autonomi[51].

L'iniziativa ha avuto successo: numerosi Stati hanno trasmesso le proprie osservazioni, tra cui l'Italia, che ha per la prima volta definito in modo relativamente chiaro la propria posizione ufficiale[52]. Quest'ultima presenta numerose convergenze con la proposta del CICR e riproduce, di fatto, un approccio *two-tier*, con alcune differenze rilevanti. In particolare, non si fa alcun riferimento alla necessità di vietare i sistemi d'arma autonomi anti-persona. Questa assenza appare tuttavia in parte compensata dal fatto che, secondo il governo italiano, un sistema d'arma può considerarsi lecito solo se la decisione ultima sull'uso della forza ("the final crucial function") – e cioè "the decision of whether or not to apply force to a previously identified and selected target" – rimane affidata a un operatore umano[53]. Nella misura in cui un sistema non può ingaggiare un obbiettivo già identificato senza l'autorizzazione di un operatore, ci si colloca chiaramente al di fuori della categoria dei sistemi autonomi propriamente detti, potendosi parlare al più di sistemi semi-autonomi.

L'affiancamento dell'Assemblea Generale al GGE come foro di discussione ha avuto dunque il duplice merito di includere nel dibattito quegli Stati che non sono parte della CCW e di contribuire, grazie al prezioso lavoro di compilazione del Segretariato, alla sistematizzazione delle posizioni emerse nel dibattito, sia individuali sia espresse nel quadro di coalizioni più ampie.

Anche a Ginevra, però, vi è uno sviluppo che vale la pena segnalare. Facciamo riferimento, in particolare, alla circolazione di un "testo in evoluzione" (*rolling text*), redatto su impulso dell'attuale chair del GGE, l'ambasciatore olandese Robert in den Bosch. Il documento è strutturato in cinque box tematici: I (definizioni), II (principi generali), III (divieti e restrizioni operative), IV (misure preventive), V (responsabilità)[54]. Nelle intenzioni del chair, questo documento mira a dare concretezza al dibattito "costringendo" le delegazioni a confrontarsi su un testo concreto, auspicabilmente destinato a confluire in un Protocollo al CCW (o in altro strumento vincolante), invece di continuare ad arrovellarsi in dibattiti inconcludenti su questioni di principio[55].

Nella sua versione più recente, il testo adotta un impianto solo parzialmente riconducibile all'approccio *two-tier*. Sotto il profilo dei divieti, infatti, ci si limita a ribadire norme la cui applicabilità ai sistemi d'arma autonomi è del tutto pacifica (ad esempio, il divieto di causare mali superflui e sofferenze inutili), mentre non vi sono riferimenti al divieto di sistemi d'arma autonomi anti-persona. Molto più interessante, invece, è la previsione del requisito del "giudizio e controllo umano appropriati al contesto", il cui contenuto è chiarito attraverso l'indicazione di una serie di misure volte a garantire tale controllo (e giudizio), tra cui la

51. *Lethal autonomous weapons systems*, 22 December 2023, UN Doc. A/RES/78/241, par. 2.
52. *Lethal autonomous weapons systems. Report of the Secretary-General*, 1 July 2024, UN Doc. A/79/88, p. 63 ss.
53. *Ivi*, p. 64.
54. GGE on LAWS, *Rolling text, status date: 12 May 2025*. I titoli dei box tematici sono stati aggiunti dall'autore sulla base del loro contenuto.
55. Si tratta di una scelta che, almeno nel breve periodo, ha già dato i suoi frutti, stimolando una discussione vivace e proficua, dopo anni di stallo (Varella 2025).

prevedibilità e tracciabilità degli effetti; la limitazione dei parametri operativi (*target*, durata, area geografica); la previsione di dispositivi di disattivazione automatica; il controllo sulle capacità di auto-apprendimento[56].

Permangono tuttavia ambiguità. Il testo non chiarisce cosa renda "appropriato" il controllo umano in un determinato contesto, né quali prerogative decisionali debbano essere assicurate agli operatori umani (mera pianificazione? Supervisione? Diritto di veto? Approvazione delle singole decisioni di *targeting*?). A questo fine, potrebbe essere utile riprendere la proposta, formulata in altra sede[57], di modulare il livello di controllo umano normativamente richiesto alla luce di tre fattori:

- *cosa* deve fare il sistema, ovvero la natura dei compiti (offensivi/difensivi) e dei target assegnati (ad esempio, obbiettivi militari per natura oppure membri di un gruppo armato di opposizione);
- *dove* verrà impiegato, ovvero le caratteristiche dell'ambiente operativo (ad esempio, presenza/assenza di civili);
- *come* funziona il sistema, ovvero le capacità senso-motorie e quelle di elaborazione delle informazioni che il sistema mette in atto per eseguire la missione assegnata (ad esempio, capacità di *swarming*, *loitering* e apprendimento automatico).

Maggiori sono le preoccupazioni etico-giuridiche sollevate dalla missione e dallo scenario operativo, più intensa sarà la forma di controllo richiesta affinché possa essere considerata "appropriata al contesto". Ad esempio, un sistema d'arma progettato per identificare civili che partecipano direttamente alle ostilità in un contesto urbano dovrà essere soggetto ad un controllo più stretto rispetto a quello previsto in relazione ad un sistema che deve intercettare missili nemici in ambiente desertico. Lo stesso dicasi per la presenza o l'assenza di caratteristiche tecniche, come quella di operare in "sciami", che possano determinare il sorgere di comportamenti "emergenti" e dunque non prevedibili. La presenza di dette caratteristiche, infatti, giustifica un controllo più stringente da parte dell'operatore umano.

7. Conclusioni

Una componente ampia e sufficientemente rappresentativa della comunità internazionale – 127 Stati, cui si aggiungono la Santa Sede e la Palestina – si è ormai pronunciata a favore dell'adozione di uno strumento giuridicamente vincolante sui sistemi d'arma autonomi[58]. Si tratta, per intenderci, di una cifra analoga a quella degli Stati parte della Convenzione sulle armi convenzionali (CCW), anche se non vi è coincidenza tra i due insiemi di Stati. A questa evoluzione si affiancano gli altri segnali positivi richiamati sopra: il graduale consolidarsi di un linguaggio comune all'interno del GGE grazie alla circolazione del *rolling text* e, sul piano più politico, l'impegno diretto del Segretario Generale delle Nazioni Unite a promuovere e facilitare la conclusione di un nuovo strumento giuridico sui sistemi d'arma autonomi entro il 2026. Tutto ciò lascia intendere che l'adozione di un trattato in materia, per quanto ancora difficile, non può più essere considerata una chimera.

Tuttavia, permangono ostacoli che non è possibile ignorare. Tra i 54 Stati che non hanno assunto una posizione chiara e, soprattutto, tra i 12 che si sono dichiarati apertamente contrari figurano numerosi Stati "militarmente significativi", secondo la terminologia del Preambolo della CCW: tra gli altri, Stati Uniti, Russia, Regno Unito, Israele, India e Australia. In tale contesto, non è escluso che l'adozione di un trattato vincolante – se e quando dovesse avvenire – possa replicare la vicenda del Trattato sulla proibizione delle armi nucleari (TPNW). Quest'ultimo, pur avendo ricevuto il sostegno iniziale di una coalizione di 138 Stati, è stato finora ratificato da poco più della metà di questi e da nessuna delle potenze nucleari, limitandone fortemente – fino quasi all'irrilevanza – l'impatto normativo.

Di fronte a questa prospettiva, e tenuto conto della profonda crisi che ormai da anni affligge il multilateralismo, vale la pena esplorare – quanto meno nel breve e medio termine – soluzioni alternative. Sotto questo aspetto, una strategia di *second best* potrebbe consistere nel promuovere l'emersione e il chiarimento delle norme indicate

56. *Rolling text*, cit., III.6.

57. Amoroso–Tamburrini 2021.

58. Maggiori informazioni sono reperibili nel sito di Automated Decision Research.

nelle pagine che precedono favorendo la convergenza progressiva su buone prassi unilaterali, formalizzate nei manuali militari nazionali di DIU. Al momento, l'unico manuale militare nazionale che contiene disposizioni specifiche sui sistemi d'arma autonomi è quello statunitense[59]. Tuttavia, altri Stati stanno attualmente aggiornando i propri manuali di DIU – tra cui l'Italia e il Regno Unito – e tale processo potrebbe offrire un'occasione preziosa per includere disposizioni analoghe, auspicabilmente ispirate all'approccio proposto dal Comitato internazionale della Croce Rossa.

Se sufficientemente omogenee, queste prassi potrebbero contribuire in misura significativa alla formazione di nuove norme consuetudinarie, colmando parzialmente il vuoto normativo e preparando il terreno per un futuro trattato. La giurisprudenza internazionale ha riconosciuto nei manuali militari una fonte rilevante per l'accertamento degli elementi costitutivi della consuetudine[60]. In questa chiave, essi non devono essere visti solo come strumenti interni di addestramento ma, in attesa di un trattato ampiamente condiviso, anche come veicoli di produzione normativa "dal basso", capaci di anticipare e orientare sviluppi giuridici futuri.

Riferimenti bibliografici

D. Amoroso (2020), *Autonomous Weapons Systems and International Law. A Study on Human-Machine Interactions in Ethically and Legally Sensitive Domains*, ESI/Nomos, 2020

D. Amoroso, G. Tamburrini (2021), *Toward a Normative Model of Meaningful Human Control over Weapons Systems*, in "Ethics & International Affairs", vol. 35, 2021, n. 2

Article36 (2013), *Killer Robots: UK Government Policy on Fully Autonomous Weapons*, April 2013

P. Asaro (2019), *What is an 'Artificial Intelligence Arms Race' Anyway?*, in "I/S: A Journal of Law and Policy for the Information Society", 2019

I. Bode, H. Huells (2022), *Autonomous Weapons Systems and International Norms*, McGill-Queen's University Press, 2022

V. Boulanin, M. Verbruggen (2017), *Mapping the Development of Autonomy in Weapon Systems,* SIPRI, 2017

E. Cannizzaro (2014), *Proportionality in the Law of Armed Conflict*, in A. Clapham, P. Gaeta (eds.), "The Oxford Handbook of International Law in Armed Conflict", Oxford University Press, 2014

C. Carpenter (2014), *"Lost" Causes: Agenda Vetting in Global Issue Networks and the Shaping of Human Security*, Cornell University Press, 2014

K. Chowdhury (2025), *Adversarial Machine Learning: Attacking and Safeguarding Image Datasets*, in "arXiv", 31 January 2025

Comitato internazionale della Croce Rossa (2024), *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts. Building a Culture of Compliance for IHL to Protect Humanity in Today's and Future Conflicts*, 2024

Comitato internazionale della Croce Rossa (2021), *Position on Autonomous Weapon Systems*, 2021

Comitato internazionale della Croce Rossa (2019), *Autonomy, artificial intelligence and robotics: Technical aspects of human control*, 2019

59. Dipartimento della Difesa USA, *Law of War Manual*, June 2015 (aggiornato nel luglio 2023), par. 6.5.9.
60. V., ad esempio, Tribunale internazionale per la ex-Jugoslavia, *The Prosecutor v. Dusko Tadić*, IT-94-1-AR72, Appeals Chamber, Decision, 2 ottobre 1995, parr. 92, 99, 108, 118, 131, 580.

D. Copeland (2025), *A Functional Approach to the Legal Review of Autonomous Weapon Systems*, Brill, 2025

B. de Vries (2023), *Individual Criminal Responsibility for Autonomous Weapons Systems in International Criminal Law*, Brill, 2023

M. Ekelhof, G. Persi Paoli (2020), *Swarm Robotics. Technical and Operational Overview of the Next Generation of Autonomous Systems*, UNIDIR, 2020

W.J. Fenrick (1982), *The Rule of Proportionality and Protocol I on Conventional Warfare*, in "Military Law Review", vol. 98, 1982

J.-M. Henckaerts, L. Doswald-Beck (2005), *Customary International Humanitarian Law*, Cambridge University Press, 2005

I. Henderson, K. Reece (2018), *Proportionality under International Humanitarian Law: The "Reasonable Military Commander" Standard and Reverberating Effects*, in "Vanderbilt Journal of Transnational Law", vol. 51, 2018, n. 3

I. Henderson, P. Keane, J. Liddy (2017), *Remote and Autonomous Warfare Systems: Precautions in Attack and Individual Accountability*, in J.D. Ohlin (ed.), "Research Handbook on Remote Warfare, Edward Elgar", 2017

J. Holland (2004), *Military Objective and Collateral Damage: Their Relationship and Dynamics*, in "Yearbook of International Humanitarian Law", vol. 7, 2004

Human Rights Watch (2025), *A Hazard to Human Rights. Autonomous Weapons Systems and Digital Decision-Making*, 28 April 2025

Human Rights Watch (2012), *Losing Humanity. The Case against Killer Robots*, 2012

N. Jevglevskaja (2018), *Weapons Review Obligation under Customary International Law*, in "International Law Studies", vol. 94, 2018

D. Kennedy (2004), *Dark Side of Virtue: Reassessing International Humanitarianism*, Princeton University Press, 2004

J. Kwik (2024), *Lawfully Using Autonomous Weapon Technologies*, Springer, 2024

M. Liu, J. Wei, Y. Liu, J. Davis (2025), *Human and AI Perceptual Differences in Image Classification Errors*, in T. Walsh, J. Shah, Z. Kolter (eds.), "Proceedings of the AAAI Conference on Artificial Intelligence", vol. 39, 2025, n. 13

S. Losey (2024), *US Air Force stages dogfights with AI-flown fighter jet*, in "Defense News", 19 April 2024

M. Mancini (2006), *Air Operations against the Federal Republic of Yugoslavia (1999)*, in N. Ronzitti, G. Venturini (eds.), "The Law of Air Warfare: Contemporary Issues", Eleven International Publishing, 2006

D. Mauri (2022), *Autonomous Weapons Systems and the Protection of the Human Person. An International Law Analysis*, Edward Elgar, 2022

T. McFarland (2020), *Autonomous Weapon Systems and the Law of Armed Conflict. Compatibility with International Humanitarian Law*, Cambridge University Press, 2020

G. Mecacci, D. Amoroso, L. Cavalcante Siebert et al. (eds.) (2024), *Research Handbook on Meaningful Human Control of Artificial Intelligence Systems*, Edward Elgar, 2024

S. Parkin (2015), *Killer robots: The soldiers that never sleep*, in "BBC news", 16 July 2015

D. Saxon (2021), *Fighting Machines: Autonomous Weapons and Human Dignity*, University of Pennsylvania Press, 2021

P. Scharre (2018), *Army of None. Autonomous Weapons and the Future of War*, W.W. Norton & Company, 2018

P. Scharre (2016), *Centaur Warfighting: The False Choice of Humans vs. Automation*, in "Temple International & Comparative Law Journal", vol. 30, 2016, n. 2

M.N. Schmitt, J.S. Thurnher (2013), *"Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict*, in "Harvard National Security Journal", 2013

A. Seixas-Nunes (2022), *The Legality and Accountability of Autonomous Weapon Systems. A Humanitarian Law Perspective*, Cambridge University Press, 2022

N.E. Sharkey (2016), *Staying the Loop: Human Supervisory Control of Weapons*, in N. Bhuta, S. Beck, R. Geiβ, et al. (eds.), "Autonomous Weapons Systems: Law, Ethics, Policy", Cambridge University Press, 2016

M.R. Taddeo, A. Blanchard (2022), *A Comparative Analysis of the Definitions of Autonomous Weapons Systems*, in "Science and Engineering Ethics", vol. 28, 2022

J.S. Thurnher (2014), *Examining Autonomous Weapon Systems from a Law of Armed Conflict Perspective*, in H. Nasu, R. McLaughlin (eds.), "New Technologies and the Law of Armed Conflict", T.M.C. Asser Press, 2014

L. Valdares Fernandes Barbosa (2025), *Autonomous Weapons Systems and the Responsibility of States. Challenges and Possibilities*, Routledge, 2025

L. Varella (2025), *Editorial: Disarmament is Always the Smartest Choice*, in "CCW Report", 2025

M. Zajac (2023), *AWS compliance with the ethical principle of proportionality: three possible solutions*, in "Ethics and Information Technology", vol. 25, 2023, n. 1

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0236 • articolo sottoposto a peer review • pubblicato in anteprima il 7 ago. 2025

Elisa Orrù

How the notion of "hybrid threat" is reshaping security. The case of migration and disinformation within the EU and its implications for the rule of law and democracy

This article examines the emergence of the concept of "hybrid threats" in EU security policy, and its implications for fundamental principles of the rule of law and democracy. It discusses these dynamics by focusing on two exemplary phenomena that have been framed as "hybrid threats": migration and disinformation. The article's main argument is that characterising these phenomena as "hybrid threats" leads to an increased intertwining of civil and military, internal and external dimensions of security, resulting in a "hybridisation" of security policies. Ultimately, this shifts the emphasis of securitisation towards the extreme pole of "existential threats". This places significant pressure on the fundamental principles of the rule of law, such as respect for fundamental rights and judicial control over executive powers, and also undermines democratic participation and the integrity of public discourse.

Hybrid threats – Security Union – Area of Freedom, Security and Justice – Disinformation – Migration Securitisation

"Minacce ibride" e ridefinizione della sicurezza. Le misure Ue nel campo della migrazione e della disinformazione e le implicazioni per lo Stato di diritto e la democrazia

L'articolo esamina l'emergere del concetto di "minacce ibride" nelle politiche di sicurezza dell'Ue e le sue implicazioni per i principi fondamentali dello Stato di diritto e della democrazia. Il saggio analizza queste dinamiche concentrandosi su due esempi emblematici di fenomeni che sono stati progressivamente e sempre più decisamente caratterizzati come "minacce ibride": la migrazione e la disinformazione. L'argomento principale dell'articolo è che definire questi fenomeni "minacce ibride" determina una crescente interconnessione tra le dimensioni civile e militare, interna ed esterna della sicurezza, con conseguente "ibridazione" delle politiche di sicurezza. In ultima analisi, tale processo sposta l'accento delle misure di sicurezza verso il polo estremo della risposta a "minacce esistenziali". Ciò esercita una pressione significativa sui principi fondamentali dello Stato di diritto, quali il rispetto dei diritti fondamentali e il controllo giudiziario sui poteri esecutivi, e rischia di compromettere la partecipazione democratica e l'integrità del dibattito pubblico.

Minacce ibride – Unione della sicurezza – Spazio di libertà, sicurezza e giustizia – Disinformazione – Migrazione Securitizzazione

The Author is Senior Researcher at the Max Planck Institute for the Study of Crime, Security and Law, Freiburg and at Freiburg University

This paper is part of the monographic section *Le due facce della rivoluzione digitale, tra emergenze e tecnologie dual-use*, a cura di Paolo Passaglia

1. Introduction

This article[1] explores the current dynamics within the field of European common security politics, arguing that there is an ongoing strong tendency towards the progressive hybridisation of internal and civil security with military and external security. This process is driven by an increasing framing of phenomena such as cyberattacks, migration and disinformation as "hybrid threats".

The article analyses in particular recent measures taken at the EU level to deal with two prototypical phenomena framed as "hybrid threats", namely the so-called "instrumentalisation of migration" and disinformation campaigns. It observes that EU measures adopted in response to these phenomena have coalesced around two key actors: the European Border and Coast Guard Agency (EBCG), commonly known as Frontex, and the European External Action Service (EEAS). In both cases, there has been increased entanglement of the internal and civil security dimensions with the external and military dimensions. This is exemplified by Frontex's strengthened cooperation with military actors such as the North Atlantic Treaty Organisation (NATO) and the allocation of critical tasks to the EEAS, the agency responsible for the EU's common external policies.

The article further considers how this shift imposes significant strain on fundamental principles of the rule of law and democracy. On the one hand, pre-existing deficiencies such as the lack of parliamentary oversight and judicial control over Frontex's actions are exacerbated by the growing "exceptionalism" that stems from framing migration as a hybrid threat. On the other hand,

1. This article's topic was first presented at the conference "Decision-Making in the Age of Emergencies: Challenges and Future Perspectives", held at Bocconi University in Milan in April 2025. I would like to thank Arianna Vedaschi and Lidia Bonifati for their kind invitation and all the participants for their valuable feedback and inspiring discussions. I would also like to thank my colleagues at the Max Planck Institute for the Study of Crime, Security and Law in Freiburg, where I presented an earlier version of the article, as well as the participants of the Centre for Security and Society's workshop on hybrid threats at Freiburg University in July 2025 for the insightful discussions on the topic.

treating disinformation as an existential threat to be addressed using military methods and logic is contrary to the concept of a democratic public sphere, which, as Hannah Arendt points out, is nourished by the exchange of differing opinions rather than the pursuit of truth.

The article proceeds as follows. Section 2 provides an overview of the historical development of a common European internal security policy area, identifying three phases of institutionalisation, algorithmisation, and hybridisation. Section 3 focuses on the ongoing third phase (hybridisation) and explores the measures taken to counteract two exemplary phenomena framed as "hybrid threats": migration and disinformation. Section 4 discusses the implications of the hybridisation of EU security for the rule of law and democracy. Finally, Section 5 concludes by summarizing the article's main arguments.

2. Three phases of European internal security: institutionalisation – algorithmisation – hybridisation

The first nucleus of today's European Union (EU) — the European Coal and Steel Community (ECSC) — was established in the aftermath of the Second World War, driven by the motivation to place the raw materials essential for waging war under the control of the Community. This was intended to discourage European states from resorting to war against each other again. Since the very beginning of the European integration process, therefore, a connection to security has been present. However, attempts to create a common defence policy were quickly abandoned in favour of transferring defence and military cooperation competences to NATO[2]. Consequently, when the Treaty of Rome, which established the European Economic Community (EEC), was signed in 1957, it focused solely on economic integration and made no provision for security cooperation, either internal or external.

However, as early as the 1970s, EEC Member States had already begun informal cooperation in matters of security. From 1976 until 1993, the interior and justice ministers of each state met twice a year at TREVI (*Terrorisme, Radicalisme et Violence Internationale*) group meetings to discuss organised crime, terrorism, police cooperation and migration[3]. An important milestone in the formalisation of security cooperation in Europe was the signing of the Schengen treaties in 1985 and 1990. After the European Commission's proposal to abolish controls at European internal borders was rejected by some Member States, a smaller group of states decided to sign international treaties outside the European Community's framework, intending to act as a catalyst for accession by further states. As the abolition of border controls between the signatory states was perceived by relevant actors as reducing security, "compensatory" measures to strengthen police and judicial cooperation, as well as the first European database — the Schengen Information System (SIS) — were introduced[4].

This first phase of European security integration culminated in the 1992 Treaty of Maastricht and the 1997 Treaty of Amsterdam, which incorporated the previously informal or intergovernmental cooperation — including the Schengen acquis — into the institutional framework of the EU and formally established the "Area of Freedom, Security and Justice" (AFSJ) as an EU policy area.

During this initial phase of European security integration, internal security was primarily presented as a necessary measure to support the implementation of the common market, particularly the four freedoms of movement of goods, services, capital and people. Security cooperation among Member States was officially regarded primarily in terms of "flanking measures" to achieve market integration and address the challenges arising from it. There were also strategic reasons for this: as the core competences transferred to European institutions were of economic nature, the connection to the realisation of the common market was central to avoiding criticism of the ECC and later EU institutions for acting *ultra vires*.

The most significant feature of this initial phase was the progressive institutionalisation of security cooperation. Practices originating from informal cooperation, such as the TREVI meetings, or from cooperation occurring outside the institu-

2. Holzhacker–Luif 2014.
3. *Ibidem*; Monar 2001.
4. Peers 2017.

tional framework of the European Communities, such as that following the Schengen treaties, were gradually incorporated into the EU. The informal and intergovernmental origins of these practices continued to shape European security cooperation even after it was transferred to the EU institutional framework. Indeed, EU security policies have long been characterised by a clear primacy of executive powers over parliamentary deliberation and judicial control[5].

The second phase of European security cooperation began around the turn of the millennium. It was characterised by strategic programmes from the European Council, including the Tampere, Hague and Stockholm programmes, and culminated in 2015 with a critical communication from the EU Commission: the "European Agenda for Security" (hereafter referred to as the "Security Agenda")[6]. During this phase, common European security measures predominantly focused on information exchange. This was given precedence over operational cooperation since security politics were still considered a core sovereign competence of individual states. By contrast, information exchange could more easily be presented as merely facilitating coordination between national agencies, despite the fact that EU initiatives also played a significant role in intensifying national security measures in practice[7].

During the second phase, a series of large databases were established, equipped with increasingly sophisticated search and analysis functions. The previously existing SIS was progressively equipped with new functionalities and flanked by the biometric database Eurodac, the Visa Information System (VIS) and, more recently, the decentralised Passenger Name Record (PNR) system. Other systems that have been established include the Entry/Exit System (EES) and European Travel Information and Authorisation System (ETIAS), expected to become operational in 2025 and 2026 respectively. During this phase, alphanumerical systems such as SIS were equipped with biometric functions and new search functionalities. Binary verification logics were complemented with risk assessment functions and interoperability between the different systems became imperative.

This second phase continued until around 2020, marking both continuity and rupture with the first phase. On the one hand, the official focus continued to be on internal or civil security measures, as opposed to external or military security measures, although a tendency to blur this distinction was starting to emerge, particularly with regard to border controls[8]. On the other hand, this second phase departed from the narrative of the first phase, according to which security cooperation within the EU was functional to maintaining the free internal market. In contrast, in this second phase, relevant national and European actors increasingly viewed enforcing security within the EU as an end in itself that did not need to be justified by its contribution to the realisation of the internal market. This meant that security could be enforced, if necessary, even at the expense of the previously prioritised freedoms of movement[9].

In addition to continuing the trend of supranationalisation that began in the first emergent phase of EU security policy, the second phase was characterised by what has been termed the "algorithmisation of security"[10]. The aforementioned expansion of the EU's large database and of information exchange was not merely a quantitative increment. Rather, it has brought about a qualitative shift from norm-based, reactive verification systems used to identify individuals already known

5. de Waele 2017; Holzhacker–Luif 2014.
6. European Commission, *The European Agenda on Security,* COM(2015) 185; European Council *The Stockholm Programme - An open and secure Europe serving and protecting the citizens*, 2 December 2009; European Council, *The Hague Programme: strengthening freedom, security and justice in the European Union*, 2005/C 53/01; European Council, *Tampere European Council 15 and 16 October 1999. Presidency Conclusions*, 1999.
7. Orrù 2022-b, 172; Orrù 2021, p. 141.
8. Poscher 2016, p. 68; Bigo 2000, p. 171, pp. 186-188.
9. Orrù 2022-b, pp. 204-206; Orrù 2021, pp. 277-283; Bellanova–de Goede 2020. Specifically on the relationship between the values of security, freedom and justice see Orrù 2022-a.
10. Bellanova–de Goede 2020. See also literature on algorithmic regulation, on which the concept of algorithmic security builds: Ulbricht 2018; Yeung 2018.

to the authorities, to investigative, risk-based, and pre-emptive tools used to identify potential "suspect" individuals who are not yet known to the authorities[11]. This new security logic, which is especially evident in the risk-based approach of the EU PNR directive and the upcoming ETIAS, aims to produce a probabilistic assessment of people's future behaviour. Under this approach, individuals are no longer evaluated based on their adherence to or violation of pre-established, relatively stable and widely recognised rules. Instead, they are profiled and sorted into risk categories based on "mobile", data-driven and opaque norms[12].

This risk-based, data-driven, pre-emptive approach to security challenges fundamental principles of the rule of law[13] and threatens to undermine anti-discrimination safeguards[14]. Moreover, it is based on an altered relationship between facts and norms, which has significant consequences for how legal and political issues are addressed by the law. At the heart of legal systems based on the rule of law is the "normative force" of the law. This lies in regulation that explicitly and transparently connects legal facts with legal consequences, providing a clear reference for legal subjects to orient their behaviour[15]. Data-driven, risk-based, pre-emptive security departs from this model as it explicitly renounces providing legal subjects with clear, stable, and intelligible norms of conduct. This deprives them not only of effective redress mechanisms[16], but also redefines the relationship between the legal and political systems and their subjects in a way that discards human autonomy. Rather than being seen as moral agents who can orient their conduct based on general and intelligible norms, subjects are now viewed as trait carriers to be profiled, rated, predicted and, if deemed appropriate, stopped[17].

Finally, while the main tendencies of the first two phases — namely, supranationalisation and algorithmisation — were still unfolding, a third tendency began to emerge. I suggest referring to this tendency as "hybridisation", as it involves an increasing connection between civil and military, internal and external security. By around the year 2020, this tendency had become the dominant feature of current developments within European security measures. The central drivers of this process are phenomena categorised as hybrid threats, such as cyberattacks, the so-called "instrumentalisation of migration" at European borders, and disinformation campaigns. As these threats blur the traditional line between the military and civil domains — so the main argument justifying this development in European security — they require an equally "hybrid" response. This third phase, its key concepts, dynamics, and challenges are the subject of the following sections.

3. The current process of hybridisation of European Security

As mentioned above, the convergence of internal and external security dimensions is not a new phenomenon, nor did it emerge abruptly. This trend has been observed by scholars since the beginning of the new millennium[18] and, as we will shortly see, has intensified since 2016. However, it seems reasonable to suggest that, since around 2020, this trend has been the driving force behind the most significant current developments in the field of EU security.

3.1. Key concepts: Security Union, collective security and hybrid threats

The strengthening of this tendency is reflected in EU strategic documents through the emergence of three key concepts: "Security Union", "collective

11. For a detailed analysis of this process, see Orrù 2022-b; Orrù 2021; Mitsilegas 2020; Mitsilegas 2015.
12. Leese 2014, p. 505; Amoore 2011, p. 31.
13. Bayamlioğlu–Leenes 2018; Hildebrandt 2018; Yeung 2018; Hildebrandt 2016.
14. Leese 2014. For the discriminatory potential of Big Data probabilistic models in general see O'Neil 2016.
15. Bayamlioğlu–Leenes 2018, p. 305. See also Raz 1977.
16. Bayamlioğlu–Leenes 2018, p. 309.
17. In more detail Orrù 2022-c. For a broader reflection on human agency and algorithmic "rule" see Frischmann–Selinger 2018; Hildebrandt–Rouvroy 2011.
18. See footnote 8 above.

security" and "hybrid threats". "Security Union" refers to the EU's responsibility to guarantee a high level of security throughout its Member States' territory. This term is not mentioned in EU primary law, but first appeared in an EU official document in the form of a communication issued by the European Commission (EC) in 2016, containing guidelines for implementing the 2015 Security Agenda[19]. As noted above, the latter document marked the culmination of the second phase of European security policy. Despite its being formally a mere "specification" of the previous document, the 2016 Commission's Communication actually initiated a transformation process. Although "AFSJ" is still the official term — and the one set out in EU primary law — to define the policy area of cooperation in security matters, it has been completely replaced by the 2016 newly introduced expression "Security Union" in EU strategic documents over time. A 2020 EC Communication on the EU Security Union Strategy (hereafter referred to as the "Security Union Strategy") is emblematic of this substitution process. This document only uses the expression "Security Union" and never mentions the AFSJ, thus formally reflecting the prioritisation of security over the values of freedom and justice that the term "AFSJ" encompassed[20].

A key idea behind the concept of a "Security Union" is the need to move away from a purely cooperative approach and towards one that aims to protect "the collective security of the Union as a whole"[21]. Conceptualising the EU as a collective security space and actor marks a departure from intergovernmental approaches. According to this new framing, security in the EU requires centralised powers for EU institutions and agencies, rather than being a matter for the cooperation of its Member States[22]. This represents a significant shift for a policy area that has traditionally formed the core of state sovereignty. This shift is all the more significant when considered alongside the call for convergence of internal and external, civil and military security. Indeed, the 2020 Security Union Strategy encourages EU institutions to cooperate closely with military organisations, including NATO, and adopt a "whole-of-society approach"[23], connecting the civil, military and political spheres closely with each other[24].

The keystone of this reframing of EU security and the core justification for its collectivisation is the concept of "hybrid threats". A hybrid threat, according to the European Commission's definition, consists of a "mixture of coercive and subversive activity, conventional and unconventional methods […], which can be used in a coordinate manner by state or non-state actors"[25]. By definition, hybrid threats blur the distinction between the internal and external, civil and military spheres. It is this indistinctness that provides the justification for "hybrid" responses: in order to effectively counteract hybrid threats, the argument goes, responses must be able to draw on and connect resources from both the internal and external, civil and military domains.

19. The expression "Security Union" was actually used once before 2016 in official ECC/EU documents, namely in the minutes of a 1991 European Parliament sitting (European Parliament, *Minutes of the Sitting of Monday, 10 June 1991*, Official Journal of the European Communities, vol. 34, 1991, p. 23). Against the backdrop of the First Gulf War, the text calls for the arms sector to become part of the common European market within the context of a "Security Union". Therefore, the expression had a different meaning in 1991 than it did in 2016. While the former referred to the "communitarisation" of armaments production, the latter designated the objective of a stronger EU policy in the field of internal and civil security.
20. European Commission, *The EU Security Union Strategy*, COM(2020) 605.
21. European Commission, *Delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union,* COM(2016) 230, p. 2.
22. On the EU as a collective security actor see Kaunert–Léonard 2023; Lucarelli–Sperling–Webber 2020; Sperling–Webber 2017.
23. European Commission, *The EU Security Union Strategy*, COM(2020) 605, p. 2.
24. Giannopoulos–Smith–Theocharidou 2021, p. 2.
25. European Commission, *The EU Security Union Strategy*, COM(2020) 605, p. 1; European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint Framework on Countering Hybrid Threats. A European Union Response*, JOIN(2016) 18, p. 2.

The following recent statement from the President of the European Commission exemplary summarises the interplay of these concepts and their mutual reinforcement in current EU politics:

> Extraordinary times call for extraordinary measures. […] To deal with the challenging way ahead, we need to switch into a preparedness mind-set. […] From *external and internal security* to energy, defence and research. From cyber, to trade, to foreign interference. Only if we have a clear and in-depth understanding of the threats, including *hybrid threats*, can we effectively contribute to *collective security*[26].

3.2. Two exemplary hybrid threats: the "instrumentalisation of migration" and disinformation campaigns

In recent strategic documents, the EC has fleshed out the notion of hybrid threats in more detail. These include, for example, the "instrumentalisation of migrants" at the EU's external borders, the misuse of artificial intelligence for cyberattacks and information manipulation, and attacks on critical infrastructure[27]. The Council of the EU has also concerned itself with hybrid threats, launching the EU Hybrid Toolbox and a plan to establish Hybrid Rapid Response Teams in 2022. The Toolbox is intended to facilitate coordinated responses to hybrid threats, potentially involving "the full mobilisation of all relevant civilian and military instruments where appropriate, drawing from external and internal policies"[28], whereas the Hybrid Rapid Response Teams are designed to support and coordinate efforts among Member States.

Beyond establishing these overarching, albeit still quite generic, measures, a series of actions have been taken at EU level to address specific "hybrid threats". The following focuses on two paradigmatic phenomena that have been categorised as hybrid threats, triggering different institutional dynamics within the EU: the "instrumentalisation of migration" and disinformation campaigns. The former has been used to describe the strategic opening of Turkey's and Belarus' borders to the EU in 2020 and 2021, respectively. This has given new impetus to the long-term securitisation of migration[29] within the EU and the expansion and strengthening of the EU's primary migration policy actor, Frontex. By contrast, reactions to disinformation campaigns have so far resulted in relatively fragmented actions that have not yet been translated into the operational strengthening of institutions and agencies comparable to that concerning Frontex. However, as we will see below, there is a clear convergence between the civil and military domains in this field as well, particularly with regard to the competencies of another EU agency: the EEAS.

Beginning with the first phenomenon, framing migration as a "hybrid threat" has intensified existing dynamics that have long characterised Frontex's development. Established in 2004 by Council Regulation[30], the EU Agency since its early days exhibited some military-like structures, such as the Frontex Situation Centre, a real-time monitoring centre operational since 2009[31]. Furthermore, from the time of its creation, Frontex has been one of the EU agencies that has grown most rapidly and massively, expanding significantly in terms of equipment, budget and personnel. Initially presenting itself as a mere facilitator of cooperation between Member States[32], Frontex

26. Speech by Ursula von den Leyen of 9 March 2025, as quoted in Sason–Monti–Olivares-Martinez 2025, emphasis added.
27. European Commission, *ProtectEU: a European Internal Security Strategy*, COM(2025) 148, p. 11; European Commission, *Seventh Progress Report on the implementation of the EU Security Union Strategy*, COM(2024) 198, p. 1.
28. Council of the EU, *A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security*, 21 March 2022, p. 22.
29. den Boer 2008; Bigo 2002.
30. Regulation (EC) No 2007/2004 of 26 October 2004 *establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union* (no longer in force).
31. Léonard 2010, p. 243.
32. Ellebrecht 2020, p. 145.

has evolved into an agency with a high degree of autonomy in relation to EU institutions, acting as a controller of Member States' capacity to enforce border control[33]. The "migration crises" of 2005–2006 and 2015–2016 were crucial in facilitating this rise. Since 2016, the tendency towards militarisation has been explicitly sustained through the formalisation of cooperation between Frontex and NATO[34].

The framing of Turkey's and Belarus' respective strategic opening of their borders to the EU in 2020 and 2021 as "hybrid threats" intersected with and further boosted this process of militarisation. Indeed, between 2021 and 2022, Frontex's Rapid Border Intervention Teams (RABITs) contributed to the militarisation of the Turkish and Belarusian borders with the EU by deploying border guards and technical tools to support operations. Following Russia's invasion of Ukraine in 2022, moreover, Frontex participated in rapid response and surveillance operations on the Ukrainian border, taking on responsibilities akin to those of a military operation[35].

These developments have led the EU migration policies to move towards the extreme pole of the securitisation continuum, characterised by "survival, existential threat, and militarisation"[36]. Combined with other unique Frontex features, such as units with direct operational capabilities (the aforementioned RABITs) and staff directly employed by the agency (rather than Member States), this makes Frontex probably the EU agency with the highest level of supranationalisation of operational capabilities. Furthermore, beyond its operational capacities at European borders, Frontex is responsible for running the border surveillance system EUROSUR and, once operational, the ETIAS database.

The second prototypical "hybrid threat", disinformation, has been tackled by EU institutions in various, and partly contradictory, ways. Firstly, the EU has recommended actions aimed at fostering transparency and pluralism in the media, as well as promoting media literacy[37]. Secondly, a co-regulation approach has been adopted, culminating in the Digital Services Act. This obliges the leading digital platforms to counter and remove "illegal content", thereby imposing duties on private commercial actors to counter disinformation. Thirdly, the EU has adopted a securitisation approach, resulting in EU actions converging around the EEAS (the EU agency coordinating the common foreign and security policy)[38]. Since 2015, the EEAS has been responsible for addressing "Foreign Information Manipulation and Interference" (FIMI), with a particular focus on Russian disinformation. Several subgroups have been set up within the EEAS to tackle disinformation, including the "East StratCom" team and the EU Hybrid Fusion Cell[39].

The names of these committees and groups clearly reflect a geopolitical security terminology and thinking. The choice of the EEAS as the main actor entrusted with countering disinformation is symptomatic of the securitisation and hybridisation processes occurring[40]. Indeed, the EEAS is the nucleus of the still embryonic military cooperation within the EU, running the few existing joint military operations at the EU level. These include the European Union Naval Force (EUNAVFOR) Operation Atalanta in the Horn of Africa and the Western Indian Ocean, as well as the EUNAVFOR Aspides Operation in the Red Sea and the Gulf of Aden, which were initiated in 2008 and 2024, respectively. It is not obvious why the EEAS was chosen as the main actor to deal with disinformation: even within the common security policy area, other EU institutions within DG Home or DG

33. Sarantaki 2023, pp. 28-34.
34. Léonard–Kaunert 2022, p. 1425.
35. Sarantaki 2023, pp. 163-166.
36. Léonard–Kaunert 2022, 1417.
37. European Commission 2018.
38. Casero-Ripollés–Tuñón–Bouza-García 2023.
39. See European External Action Service, *Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)*.
40. Casero-Ripollés–Tuñón–Bouza-García 2023, p. 7.

Justice, for instance, could have provided closer links to EU actors who have long experience of dealing with disinformation, such as journalists, fact-checkers and media activists[41].

The EU's approach to disinformation has thus been characterised by a twofold process of securitisation. It has first been framed as a security issue, and secondly, within the securitisation spectrum and specifically through its classification as a hybrid threat, it has been allocated to the domain of external and military security. In this context, it is important to note that disinformation emerged in Europe as a politically preeminent issue ahead of the 2019 European elections and again during the 2020-21 COVID-19 pandemic. In both cases, as reflected in the High-Level Group's 2018 report on fake news and disinformation online, disinformation was not primarily considered a security issue. Indeed, the Group's 2018 report emphasises the need for measures to enhance the transparency of online news, promote media literacy, support users and journalists, and protect media pluralism — all of which have very little connection to security policy[42].

3.3. The parallel processes of securitisation and hybridisation in the fields of migration and disinformation

We can now draw an interim conclusion from the above analysis of the two prototypical hybrid threat phenomena. In both cases, two tendencies have subsequently developed in each field, running in parallel.

Firstly, the relevant phenomena have been categorised as a security issue. This is the classic securitising process that has long been observed and analysed in the field of migration, but has only recently emerged in connection with disinformation[43]. For both phenomena, this framing in terms of security issues is the result of actions taken by relevant political actors, rather than being something inherent to the phenomena themselves. During the post-Second World War economic growth in some European countries, for example, human mobility and immigration were mostly considered in economic terms, as a needed workforce to sustain the growing economy. As we have just seen, similarly, disinformation was initially considered a matter potentially affecting democratic processes and public health policies. Securitisation processes have progressively strained these earlier understandings. For example, migrants have increasingly been depicted as "criminals", resulting in a series of connected discourses and policies that have shaped several European states' approaches to migration for decades. In the case of disinformation, the initial securitisation has occurred more recently and at a less visible level, for example through legislation that criminalises the spread of disinformation within national states[44].

The second tendency, which has stepped in on top of, or in connection with, the first securitisation step, is specifically brought about by framing the phenomena as "hybrid threats". This second step moves issues along the securitisation spectrum towards militarisation and has prompted the current process of hybridisation of security within EU policy, namely the convergence of civil and military, internal and external security. While the two steps are clearly separated in the case of migration, with an initial long period of securitisation followed more recently by a "hybridisation" phase, in the case of disinformation the two processes occurred almost simultaneously. In both cases, this second step has involved closer interlinking of internal and external, civil and military domains in EU policy – in short, a "hybridisation" of EU security.

4. Implications for the rule of law and democracy

Overall, the above developments, which integrate an ongoing securitisation process with the hybridisation of internal and external security, put

41. *Ivi*, p. 6.
42. European Commission 2018.
43. On securitisation in general, see Buzan–Wæver 2003, p. 71. On the securitisation of migration see exemplarily Léonard–Kaunert 2022; den Boer 2008; Bigo 2002. On the securitisation of disinformation Casero-Ripollés–Tuñón–Bouza-García 2023.
44. For an overview of newly introduced criminal provisions against disinformation and related acts such as deepfakes in EU States see Bleyer-Simon–Horowitz–Botan et al. 2025.

considerable pressure on the rule of law and basic democratic principles. Securitisation itself tends towards exceptionalism, namely the lowering of power-restricting mechanisms under the guise of a state of emergency. The process of hybridisation adds further intensity to this trend. The opening of von der Leyen's aforementioned speech ("Extraordinary times call for extraordinary measures") is a particularly effective example of this justification strategy.

The dynamics at work within the two fields of action addressing the two prototypical hybrid threats illustrate the mechanisms at play. Both Frontex and the European External Action Service are decentralised EU agencies which, by virtue of this, already enjoy a great margin of autonomy from EU institutional control. Within Frontex's Management Board, for example, the Commission has only two representatives who can easily be outvoted by the national representatives, while the EU Parliament representatives have no voting rights. In principle, the Court of Justice of the EU (CJEU) would have jurisdiction over Frontex's actions, but it has so far systematically avoided its responsibility by highlighting the Agency's "mere coordinating" function[45]. However, as we have seen above, Frontex has gained considerable operative power over time, making the CJEU's stance increasingly untenable. Furthermore, Frontex has been tasked with running the ETIAS, the latest European database, which is expected to become operational in 2026. ETIAS will be based on travellers' risk assessment, a pre-emptive security approach which, as we have seen, is fundamentally at odds with the rule of law[46]. This makes it more urgent than ever to impose stronger accountability, democratic scrutiny, and effective judicial control over the agency. Against this backgorund, framing and addressing migration as a hybrid threat is more likely to hinder than facilitate this desirable development. Moreover, the problem, although exacerbated by the existing lack of controls over Frontex, is not confined to this agency. National states are also increasingly framing migration as a hybrid attack to justify the infringement of basic human rights[47].

Whilst the framing of migration as a hybrid threat primarily poses problems in terms of the rule of law, dealing with disinformation as a hybrid threat especially puts pressure on democratic principles. Paradoxically, the main cause for concern regarding disinformation is its potential to disrupt democratic processes and discourses. However, classifying disinformation as a hybrid threat could undermine the very principles that should be safeguarded. As Hannah Arendt insightfully argued, claims to absolute "truth" and validity are contrary to the essence of political discourse. The political sphere thrives on debate, discussion and the exchange of opinions. On the other hand, Arendt also observed that all very different opinions must have a place in political discourse and are legitimate as long as they respect the integrity of the facts to which they refer[48]. As Arendt reminds us, protecting the democratic sphere by ensuring participation in public discourse and the exchange of diverse opinions, while anchoring these in the integrity of facts, is an arduous task requiring a nuanced approach in which criticism, openness, and diversity of opinion are essential. Exceptionalism and existential threats, on the other hand, are the most effective ways to silence criticism and differing opinions. Therefore, it is highly unlikely that democracy can be best defended under the banner of fighting "hybrid threats".

5. Conclusion

This article examined the increasing tendency within the EU to categorise issues as "hybrid threats" and investigated the impact of this on security understanding and practices. It analysed the cases of migration and disinformation in particular. Once these phenomena had been "securitised", meaning they were declared and dealt with as security problems, the hybridisation of security shifted EU measures in this area towards the "existential threat" extreme by interlacing the civil/internal and military/external spheres. These developments exacerbate the existing problems of lack of accountability and democratic control within the EU, making the need to strengthen power-restricting mechanisms and democratic participation more urgent than ever.

45. De Coninck 2023.
46. Specifically on Frontex and ETIAS see Thönnes–Vavoula 2023; Eklund 2022.
47. Bücker–Möller 2025.
48. Arendt 1964/2013, pp. 23-27.

References

L. Amoore (2011), *Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times*, in "Theory, Culture & Society", vol. 28, 2011

H. Arendt (1964/2013), *Wahrheit und Lüge in der Politik: Zwei Essays*, Piper Taschenbuch, 2013

E. Bayamlioğlu, R. Leenes (2018), *The 'rule of law' implications of data-driven decision-making: a techno-regulatory perspective*, in "Law, Innovation and Technology", vol. 10, 2018

R. Bellanova, M. de Goede (2020), *The Algorithmic Regulation of Security: An Infrastructural Perspective*, in "Regulation & Governance", 2020

D. Bigo (2002), *Security and Immigration: Toward a Critique of the Governmentality of Unease*, in "Alternatives 27", Special Issue, 2002

D. Bigo (2000), *When two become one: Internal and external securitisations in Europe*, in "International Relations Theory and the Politics of European Integration", Routledge, 2000

K. Bleyer-Simon, M.A. Horowitz, M. Botan et al. (2025), *How Is Disinformation Addressed in the Member States of the European Union? – 27 Country Cases*, in "European Digital Media Observatory", 2025

J. Bücker, L.S. Möller (2025), *Beyond Derogation: Context-Driven Interpretation of Migrants' Rights and the Risks of Circumventing Article 15 ECHR*, in "Max Planck Institute for Comparative Public Law & International Law (MPIL) Research Paper", vol. 6, 2025

B. Buzan, O. Wæver (2003), *Regions and Powers: The Structure of International Security*, Cambridge University Press, 2003

A. Casero-Ripollés, J. Tuñón, L. Bouza-García (2023), *The European Approach to Online Disinformation: Geopolitical and Regulatory Dissonance*, in "Humanities and Social Sciences Communications", vol. 10, 2023

J. De Coninck (2023), *Shielding Frontex*, in "Verfassungsblog", September 2023

H. de Waele (2017), *Entrenching the Area of Freedom, Security and Justice. Questions of institutional governance and judicial control*, in M. Fletcher, E. Herlin-Karnell, C. Matera (eds.), "The European Union as an Area of Freedom, Security and Justice", Routledge, 2017

M. den Boer (2008), *Immigration and its Effect on the Security Discourse in Europe: Time for Demystification*, in "Amsterdam Law Forum", vol. 1, 2008, n. 1

A.M. Eklund (2022), *Frontex and 'Algorithmic Discretion' (Part I): The ETIAS Screening Rules and the Principle of Legality*, in "Verfassungsblog", September, 2023

S. Ellebrecht (2020), *Mediated Bordering:* EUROSUR*, the Refugee Boat, and the Construction of an External EU Border*, transcript publishing, 2020

European Commission (Directorate-General for Communications Networks, Content and Technology) (2018), *A Multi-Dimensional Approach to Disinformation: Report of the Independent High Level Group on Fake News and Online Disinformation*, Publications Office, 2018

B. Frischmann, E. Selinger (2018), *Re-Engineering Humanity*, Cambridge University Press, 2018

G. Giannopoulos, H. Smith, M. Theocharidou (2021), *The Landscape of Hybrid Threats: A Conceptual Model (Public Version)*, Publications Office of the European Union, 2021

M. Hildebrandt (2018), *Algorithmic regulation and the rule of law*, in "Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences", vol. 376, 2018

M. Hildebrandt (2016), *Law as Information in the Era of Data-Driven Agency*, in "The Modern Law Review", vol. 79, 2016, n. 1

M. Hildebrandt, A. Rouvroy (eds.) (2011), *Law, Human Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology*, Routledge, 2011

R.L. Holzhacker, P. Luif (2014), *Introduction: Freedom, Security and Justice after Lisbon*, in Id. (eds.), "Freedom, Security, and Justice in the European Union: Internal and External Dimensions of Increased Cooperation after the Lisbon Treaty", Springer, 2014

C. Kaunert, S. Léonard (2023), *Collective securitization and crisification of EU policy change two decades of EU counterterrorism policy*, Routledge, 2023

M. Leese (2014), *The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union*, in "Security Dialogue", vol. 45, 2014, n. 5

S. Léonard (2010), *EU border security and migration into the European Union: FRONTEX and securitisation through practices*, in "European Security", vol. 19, 2010, n. 2

S. Léonard, C. Kaunert (2022), *The securitisation of migration in the European Union: Frontex and its evolving security practices*, in "Journal of Ethnic and Migration Studies", vol. 48, 2022, n. 6

S. Lucarelli, J. Sperling, M. Webber (eds.) (2020), *Collective Securitisation and Security Governance in the European Union*, Routledge, 2020

V. Mitsilegas (2020), *The Preventive Turn in European Security Policy: Towards a Rule of Law Crisis?*, in F. Bignami (ed.), "EU Law in Populist Times: Crises and Prospects", Cambridge University Press, 2020

V. Mitsilegas (2015), *The Transformation of Privacy in an Era of Pre-emptive Surveillance*, in "Tilburg Law Review", vol. 20, 2015, n. 1

J. Monar (2001), *The Dynamics of Justice and Home Affairs: Laboratories, Driving Factors and Costs*, in "JCMS: Journal of Common Market Studies", vol. 39, 2001, n. 4

C. O'Neil (2016), *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown Publishers, 2016

E. Orrù (2022-a), *Freedom, security and justice in the European Union: a short genealogy of the "Security Union"*, in "Eunomia. Rivista di studi su pace e diritti umani", 2022, n. 1

E. Orrù (2022-b), *Legittimità e digitalizzazione. Per una critica realistica delle politiche di sicurezza dell'Unione europea*, Wolters Kluwer, 2022

E. Orrù (2022-c), *The European PNR Directive as an Instance of Pre-Emptive, Risk-Based Algorithmic Security and Its Implications for the Regulatory Framework*, in "Information Polity", vol. 27, 2022, n. 2

E. Orrù (2021), *Legitimität, Sicherheit, Autonomie. Eine philosophische Analyse der EU-Sicherheitspolitik im Kontext der Digitalisierung*, Nomos, 2021

S. Peers (2017), *The rise and fall of EU justice and home affairs law*, in M. Fletcher, E. Herlin-Karnell, C. Matera (eds.), "The European Union as an Area of Freedom, Security and Justice", Routledge, 2017

R. Poscher (2016), *Tendencies in Public Civil Security Law*, in "European Journal for Security Research", vol. 1, 2016

J. Raz (1977), *The rule of law and its virtue*, in "Law Quarterly Review", vol. 93, 1977

A. Sarantaki (2023), *Frontex and the rising of a new border control culture in Europe*, Routledge, Taylor & Francis Group, 2023

E. Sason, C. Monti, P. Olivares-Martinez (2025), *Security – A Firm Construct or an Undetermined Concept?*, in "eucrim", 2025, n. 1

J. Sperling, M. Webber (2017), *NATO and the Ukraine Crisis: Collective Securitisation*, in "European Journal of International Security", vol. 2, 2017, n. 1

C. Thönnes, N. Vavoula (2023), *Automated Predictive Threat Detection after Ligue Des Droits Humains: Implications for ETIAS and CSAM (Part II)*, in "Verfassungsblog", 2023

L. Ulbricht (2018), *When Big Data Meet Securitization. Algorithmic Regulation with Passenger Name Records*, in "European Journal for Security Research", vol. 3, 2018

K. Yeung (2018), *Algorithmic Regulation: A Critical Interrogation*, in "Regulation & Governance", vol. 12, 2018

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0240 • articolo sottoposto a peer review • pubblicato in anteprima il 28 ott. 2025

Lidia Bonifati

Droni ed emergenze: quali sfide per il costituzionalismo?

I droni sono sempre più spesso utilizzati nei contesti di emergenza di natura tanto politica quanto tecnica. Infatti, al di là dell'uso dei droni nei conflitti armati e nelle operazioni di contrasto al terrorismo, esperienze recenti mostrano che questi sono impiegati sempre più spesso anche nella gestione di altre emergenze, come quella sanitaria, climatica, migratoria e umanitaria. Per quanto i droni offrano grandi opportunità nei contesti emergenziali, il presente contributo mostra che l'uso dei droni solleva notevoli sfide per i principi cardine del costituzionalismo. L'analisi si concentra in particolare sul principio di trasparenza, il principio di eguaglianza, la tutela dei diritti fondamentali e le forme di controllo, facendo riferimento all'esperienza statunitense e a quella europea.

Costituzionalismo – Controllo giurisdizionale – Diritti fondamentali – Droni – Emergenze

Drones and Emergencies: What Challenges for Constitutionalism?

Drones are increasingly used in emergency situations, both political and non-political. In fact, beyond their use in armed conflicts and counter-terrorism operations, recent experiences show that drones are increasingly being used in the management of other emergencies, such as health, climate, migration and humanitarian crises. Although drones offer great opportunities in emergency situations, this article shows that their use raises significant challenges for the core principles of constitutionalism. The analysis focuses in particular on the principle of transparency, the principle of equality, the protection of fundamental rights, and constitutional review, with reference to the US and European experience.

Constitutionalism – Judicial review – Drones – Fundamental rights – Emergencies

L'Autrice è assegnista di ricerca in Diritto pubblico comparato presso l'Università Commerciale "Luigi Bocconi"

Questo contributo fa parte della sezione monografica *Le due facce della rivoluzione digitale, tra emergenze e tecnologie* dual-use, a cura di Paolo Passaglia

Si ringrazia il finanziamento del MIUR-PRIN Bando 2020 – prot. 2020M47T9C "Decision-Making in the Age of Emergencies: New Paradigms in Recognition and Protection of Rights". L'autrice desidera ringraziare la prof.ssa Arianna Vedaschi e il prof. Paolo Passaglia per i preziosi consigli sulle bozze preliminari dell'articolo. Trattandosi di temi in costante evoluzione, si specifica che l'analisi è aggiornata al 25 settembre 2025

1. Introduzione

L'uso sempre più massiccio dei droni nei conflitti armati, come dimostrato dal conflitto in corso in Ucraina, ha contribuito a riaprire il dibattito sulla portata rivoluzionaria (o meno) dei droni nelle dinamiche delle guerre[1] e sull'uso dei droni non solo a scopo militare ma anche umanitario[2]. I droni impiegati nel conflitto russo-ucraino sono infatti un esempio efficace per comprendere il concetto di tecnologia c.d. *dual-use*, ossia una tecnologia che può essere utilizzata a fini tanto militari quanto civili e umanitari[3]. Da un lato, le forze armate russe hanno impiegato droni militari fin dall'inizio della guerra, lanciando imponenti attacchi di "sciami di droni"[4] contro i propri obiettivi in Ucraina[5] e, più recentemente, violando gli spazi aerei di alcuni Stati Membri della NATO sul confine ucraino[6]. Anche le forze di Kyiv hanno ricorso all'uso di droni, inizialmente con attacchi sporadici in territorio russo, fino ad arrivare all'operazione "Spider's Web" con cui, lo scorso 2 giugno 2025, 117 droni ucraini hanno attaccato cinque basi militari russe e danneggiato diversi bombardieri strategici[7]. Dall'altro

1. Si vedano per esempio Kreps–Lushenko 2023 e Kunertova 2023.
2. Wilder 2022.
3. Sulle tecnologie *dual use*, si vedano Alic 1994; Forge 2010; Miller 2018; Pustovit–Williams 2010.
4. Sull'intensità degli attacchi di droni russi in Ucraina, si veda quanto ricostruito da Ali–Duggal 2025.
5. L'uso dei droni russi è talmente pervasivo che il Consiglio per i Diritti Umani delle Nazioni Unite ha recentemente pubblicato un'inchiesta in cui emerge l'uso sistematico dei droni per operazioni di targeting di civili a Kherson (Human Rights Council 2025).
6. Il riferimento è a quanto avvenuto in Polonia il 9 settembre 2025 e in Romania il 13 settembre 2025 (cfr. Charlish–Kelly–Erling 2025; Casey–Boyd 2025; Kayali 2025). Sempre in riferimento agli spazi aerei dei Paesi NATO, è importante segnalare che, il 22 settembre 2025, l'avvistamento di diversi droni non identificati ha comportato la chiusura di alcuni aeroporti danesi e norvegesi, per quanto non sia stato accertato il coinvolgimento russo (cfr. BBC News 2025).
7. Cfr. Adams–Lukiv 2025.

lato, il conflitto in Ucraina ha riportato l'attenzione su un ulteriore uso dei droni nei teatri di guerra, ossia droni non armati impiegati a scopo umanitario dalle organizzazioni nazionali e internazionali presenti sul campo, in particolare per le operazioni di ricerca e soccorso dei superstiti dopo i bombardamenti[8]. Pertanto, il riferimento al caso ucraino è particolarmente utile per descrivere una tendenza che vede i droni sempre più spesso utilizzati nei contesti di emergenza di natura tanto politica quanto tecnica[9]. Infatti, al di là della presenza sempre più pervasiva dei droni nei conflitti armati e nelle operazioni di controterrorismo, diverse esperienze recenti dimostrano che questi sono impiegati anche nella gestione di altre emergenze, come quella sanitaria, climatica, migratoria e umanitaria.

Il dibattito scientifico sui droni nelle emergenze si è sviluppato inizialmente nell'ambito delle relazioni internazionali e della geopolitica. Infatti, il crescente uso dei droni militari da parte di attori statali e non-statali pone non pochi problemi in termini di sicurezza internazionale e/o regionale, in quanto la proliferazione dei droni potrebbe innescare o aggravare dinamiche di destabilizzazione in aree già fragili[10]. Al dibattito si è aggiunta in seguito un'ulteriore prospettiva di ricerca, questa volta di natura giuridica, grazie al contributo del diritto internazionale umanitario, del diritto penale internazionale e della filosofia del diritto. Queste branche del diritto si occupano del tema già da tempo, studiandone in particolare i profili di responsabilità penale[11] e di compatibilità con i principi del diritto internazionale umanitario e della *just war theory*[12]. Tale ambito di ricerca è stato alimentato soprattutto da un uso dei droni ormai tristemente noto, ossia per i *targeted killings* nelle operazioni di controterrorismo[13]. Da questo primo quadro è possibile notare che la prospettiva del diritto pubblico e del diritto comparato sulle problematiche legate all'uso dei droni nelle emergenze costituisce una nicchia ancora poco esplorata[14]. Tuttavia, il settore ha fornito un prezioso contributo sulla cornice teorica in cui si inserisce il tema dei droni nelle emergenze, come il costituzionalismo

8. Per una ricostruzione sui droni umanitari, sia consentito il rinvio a Bonifati 2025.
9. Si riprende in questa sede la distinzione tra emergenze politiche ed emergenze tecniche operata da Vedaschi. Le emergenze politiche includono le molteplici declinazioni assunte dalle crisi di natura bellica (ad es., guerre, rivoluzioni, colpi di Stato, insurrezioni, terrorismo internazionale, guerre ibride). Le emergenze tecniche, invece, ricomprendono quelle situazioni emergenziali determinate da eventi naturali o sociali e che pongono problemi di tutela dell'incolumità e sicurezza della popolazione (ad es., crisi finanziarie, economiche, ambientali, sanitarie, epidemie, disastri naturali) (Vedaschi 2007, p. 266 ss.). In questo contributo, si faranno rientrare nelle emergenze tecniche anche le emergenze umanitarie e migratorie, per quanto il legame che queste situazioni emergenziali spesso hanno con i contesti di conflitto (e quindi con emergenze politiche) le renda talvolta di difficile classificazione. Sulle divere categorie di emergenze, si rimanda anche a Piergigli 2023, p. 11 ss. e Pizzorusso 1993, p. 552 ss.
10. Kreps–Maxey 2021; Gilli–Gilli 2016.
11. Sul punto si vedano Amoroso 2024; Amoroso–Giordano 2019; Amoroso–Tamburini 2019; Cucco-Mauri 2018; Di Nucci–Santoni de Sio 2016; McFarland-McCormack 2014; McFarland 2020; Meloni–Patten–Borello et al. 2019.
12. Per alcuni riferimenti più generali sull'impatto dei droni (militari e civili) sul diritto internazionale umanitario e sui relativi risvolti etici, si rimanda ad Asaro 2020; Bergen–Rothenberg 2014; Blanchard–Novelli–Floridi–Taddeo2024; Chengeta 2021; Custers 2016; Enemark 2021; Galliott–MacIntosh–Ohlin 2021; Nasu–McLaughlin 2014; Saxon 2013; Taddeo 2024.
13. Sulle implicazioni etico-giuridiche dei *targeted killings* si consigliano Anderson–Waxman 2019; Boyle 2015; Brooks 2014; Casey-Maslen–Homayounnejad–Stauffer–Weizmann 2018; Cortright–Fairhust–Wall 2015.
14. Si segnala il recente volume di Frau 2024, dedicato ai sistemi d'arma autonomi nel diritto pubblico, e i lavori di Flaherty 2015 e Weaver 2021, focalizzati sul contesto statunitense.

digitale[15], la disciplina dell'intelligenza artificiale[16] e il ruolo del diritto costituzionale nelle emergenze[17]. Lo sguardo del diritto pubblico comparato risulta di estrema rilevanza nel dibattito, poiché l'uso dei droni nelle emergenze solleva diverse problematiche giuridiche che impattano direttamente su alcuni capisaldi del costituzionalismo, a partire dalla tutela dei diritti.

Il presente studio si propone di analizzare tali criticità sotto la lente del costituzionalismo, al fine di evidenziare il contributo del diritto pubblico comparato nel comprendere un fenomeno complesso. Innanzitutto, l'articolo passa in rassegna i principali contesti emergenziali che hanno visto l'impiego di droni, sottolineandone il carattere *dual-use* (par. 2). Successivamente, l'analisi si concentra sulle implicazioni che tale "doppio uso" dei droni ha sul costituzionalismo. Come emerge dall'analisi, le enormi potenzialità offerte dei droni si scontrano inevitabilmente con la necessità di rispettare principi cardine come il principio di trasparenza (par. 3) e di eguaglianza (par. 4), la tutela dei diritti fondamentali (par. 5) e adeguate forme di controllo (par. 6). Nel paragrafo conclusivo, si rifletterà inoltre sulle prospettive di regolamentazione e sul ruolo del diritto pubblico comparato nell'affrontare le sfide per il costituzionalismo sollevate dall'uso dei droni.

2. Breve panoramica sull'uso dei droni nelle emergenze

Negli ultimi decenni, gli "aeromobili a pilotaggio remoto" (c.d. droni) hanno assunto una crescente rilevanza nella condotta della guerra aerea, permettendo una partecipazione diretta alle ostilità anche da notevoli distanze dal luogo del conflitto[18]. Nonostante i droni siano comunemente associati agli omicidi mirati (c.d. *targeted killings*) compiuti dagli Stati Uniti nelle operazioni di controterrorismo a partire dai primi anni Duemila, è opportuno ricordare che i droni erano già stati impiegati a scopo militare in altri teatri di conflitto. Essi fecero la prima comparsa durante la guerra del Vietnam e, nonostante non fossero (ancora) armati, l'esercito statunitense li utilizzò per migliaia di voli di ricognizione e verso la fine del conflitto alcuni di questi furono anche dotati di missili[19]. Da quel momento in poi, i droni militari statunitensi diventarono parte integrante delle operazioni aeree nelle guerre che vedevano coinvolti gli Stati Uniti, a partire dalla guerra del Golfo e in Kosovo negli anni Novanta e poi successivamente in Iraq. Un altro Stato che ha fatto uso di droni nei conflitti armati è Israele, a partire dagli anni Settanta e Ottanta durante la guerra del Kippur e l'invasione del Libano[20]. In anni più recenti, Stati come Regno Unito, Italia, Russia, Cina e Turchia hanno dato inizio a programmi di sviluppo e produzione di droni militari, nonostante non abbiano ancora raggiunto gli standard statunitensi, sia in termini militari che tecnologici[21].

Se da un lato l'uso dei droni militari nei conflitti bellici e nelle operazioni di controterrorismo è molto noto, l'utilizzo dei droni nelle emergenze tecniche (cioè quelle di natura sanitaria, climatica, migratoria, umanitaria) ha ricevuto un'attenzione ancora limitata[22]. Le opportunità offerte dai droni c.d. umanitari sono piuttosto evidenti: hanno la capacità di raggiungere aree altrimenti isolate; possono fornire in diretta immagini sul campo; sono efficienti e precisi;

15. Cfr. Fasan 2024; Longo–Pin 2023; Quintavalla–Temperman 2023; De Gregorio 2022; Micklitz–Pollicino–Reichman 2021.
16. Cfr. Bresciani–Palmirani 2024; Dimatteo–Poncibò–Cannarsa 2022; Donati–Finocchiaro–Paolucci–Pollicino 2025; Marchetti–Parona 2022; Nardocci 2024; Stradella 2022; Vedaschi–Graziani 2025.
17. Tra i contributi più recenti, si segnalano Delledonne 2023; Piergigli 2023; Vedaschi 2024, mentre per alcuni lavori più specifici su emergenze politiche e diritto costituzionale, si rimanda a Bassu 2010; Bonetti 2006; de Vergottini 2004; Vedaschi 2022.
18. Ronzitti 2019, p. 275 ss., 322 ss.
19. Solis 2016, p. 547.
20. *Ibidem*.
21. Sullo stato dell'arte Calcagno–Marrone 2023; Dorsey–Amaral 2022.
22. Si vedano in particolare Tarr–Perera–Chahl et al. 2022; Rejeb–Rejeb–Simske–Treiblmaier 2021; Van Wynsberghe–Comes 2020; Emery 2016; Whetham 2015.

e soprattutto riducono notevolmente il rischio per gli operatori umani impegnati sul campo. I droni potrebbero essere utilizzati in operazioni pericolose, come ad esempio la ricerca di mine inesplose, la disinfezione di aree contaminate da virus e l'individuazione di superstiti o dispersi in condizioni critiche. Nei contesti di emergenza, i droni potrebbero espandere notevolmente la tutela dei diritti fondamentali, a partire dal diritto alla vita, senza mettere a rischio gli operatori umanitari. Senza soffermarci sui dettagli tecnici dei droni utilizzati nelle emergenze tecniche, che a seconda delle caratteristiche consentono varie tipologie di operazioni, è utile ricordare che i droni sono già stati usati in passato per il monitoraggio degli argini dei fiumi a rischio esondazione, per il trasporto di cibo, acqua, medicinali, riserve di sangue e vaccini in aree isolate, oltre che in missioni di ricerca e soccorso. Per esempio, durante la pandemia da Covid-19, i droni sono stati utilizzati per il trasporto di farmaci e beni essenziali in zone isolate[23]. Un ulteriore utilizzo ha riguardato il monitoraggio delle zone a rischio di eventi climatici estremi, come la mappatura degli incendi negli Stati Uniti[24], e le operazioni di tutela dell'ambiente e della biodiversità[25]. Inoltre, i droni vengono impiegati da Frontex per il controllo dei confini europei e dei flussi migratori nel Mediterraneo[26]. Allo stesso modo, alcune divisioni del Dipartimento della Sicurezza Interna degli Stati Uniti usano i droni per il pattugliamento dei confini con il Messico e con il Canada[27]. Infine, i droni sono utilizzati sempre di più nelle missioni umanitarie da organizzazioni internazionali quali le Nazioni Unite e l'Organizzazione Mondiale della Sanità, così come da organizzazioni umanitarie come il Comitato Internazionale della Croce Rossa e Medici Senza Frontiere. Esempi concreti includono le operazioni umanitarie in seguito ai terremoti di Haiti nel 2010[28], le missioni ONU di *peacekeeping* nella Repubblica Democratica del Congo, Mali e Chad[29], e più recentemente nel conflitto in corso in Ucraina.

Le sfide giuridiche che nascono dall'uso dei droni nelle emergenze risultano particolarmente articolate a causa dell'intreccio tra l'elemento tecnico (la "tecnologia drone") e di quello circostanziale (l'emergenza). In primo luogo, come già menzionato, i droni si qualificano come tecnologia *dual-use*, ossia utilizzabile tanto a scopo militare quanto civile e umanitario, e in quanto tali pongono problematiche diverse a seconda della finalità perseguita. In secondo luogo, esiste ormai un'ampia varietà di droni, con differenze sostanziali in termini di capacità e dotazioni tecnologiche. Ciò costituisce un elemento giuridicamente rilevante in quanto alcune delle criticità derivano non solo dal fatto che i droni sono dotati di sensori e telecamere attraverso cui possono raccogliere enormi quantità di dati, ma anche dal fatto che alcuni di questi sono dotati anche di tecnologie di intelligenza artificiale (e in quanto tali sono considerabili "sistemi di AI"). In terzo luogo, il fatto che i droni siano utilizzati in situazioni emergenziali è anch'esso un dato rilevante sotto il profilo giuridico in quanto si inserisce nel più ampio quadro degli stati di emergenza, in cui l'ordinamento può giustificare la limitazione di determinati diritti e libertà in base al principio di necessità[30]. Pertanto, l'intrecciarsi di tutti questi elementi dà origine a sfide che riguardano i pilastri del costituzionalismo contemporaneo. I paragrafi successivi evidenzieranno in particolare come queste impattano sul principio di trasparenza, sul principio di eguaglianza, sulla tutela dei diritti fondamentali e sulle forme di controllo.

3. Droni e principio di trasparenza

L'uso dei droni nelle emergenze, che siano conflitti armati, operazioni di controterrorismo, o missioni

23. Mohsan–Zahr–Khan et al. 2022.
24. Questo è il caso dello Stato della California, che già dal 2015 utilizza i droni per la ricognizione delle aree interessate dagli incendi a supporto dei vigili del fuoco.
25. Bayomi–Fernandez 2023; Rohi–Ejofodomi–Ofualagba 2020.
26. Csernatoni 2018.
27. Koslowski–Schulzke 2018.
28. Cfr. Emery 2016, p. 155 ss.
29. Okpaleke–Nwosu–Okoli–Olumba 2023; Fardoulis–Depreytere–Sauvage–Gallien 2019.
30. Sugli stati di emergenza, si vedano anche Ackerman 2004; Dyzenhaus 2012.

umanitarie, presenta diversi profili di complessità per quanto riguarda il rispetto del principio di trasparenza.

In tal senso, il caso più emblematico (e, forse, più problematico) è rappresentato dall'assenza di trasparenza nei processi decisionali che hanno portato all'adozione della pratica dei *targeted killings* a mezzo drone da parte degli Stati Uniti durante la *war on terror* successiva agli attacchi dell'11 settembre. Trattandosi di una scelta inerente alla sicurezza nazionale, le informazioni riguardanti il processo decisionale, per esempio relativo all'individuazione dei *target* e al ricorso a una misura di controterrorismo estrema come l'omicidio mirato, sono state a lungo inaccessibili poiché riservate. Eppure, tale livello di segretezza ha coinvolto anche la base giuridica su cui erano giustificate tali decisioni, mettendone in discussione la legittimità e costituzionalità. Ciò è diventato critico in particolare nei casi in cui si è dovuto accertare se fossero legittimi o meno i *targeted killings* compiuti in Stati terzi oppure contro cittadini statunitensi sospettati di essere parte di organizzazioni terroristiche[31]. La generale riluttanza dell'amministrazione statunitense nel fornire maggiori informazioni sulle motivazioni dietro all'individuazione dei *target* e alle successive uccisioni ha portato diverse organizzazioni, come la American Civil Liberties Union (ACLU), Human Rights Watch e Amnesty International a chiedere maggiore trasparenza così da garantire il diritto dei cittadini degli Stati Uniti di conoscere la base giuridica su cui poggia un esercizio di potere così sostanziale da portare alla privazione del diritto alla vita senza alcuna forma di *due process*[32].

Tuttavia, anche i droni utilizzati nelle emergenze tecniche pongono diversi problemi in termini di trasparenza. In primo luogo, la trasparenza riguarda l'accesso ai dati raccolti dai droni e al trattamento che ne viene fatto. Infatti, si tratta di informazioni che non necessariamente sono accessibili agli individui coinvolti dalle operazioni dei droni che monitorano un'area urbana colpita da un disastro naturale o che raccolgono immagini per la ricerca di superstiti[33]. Inoltre, quando il drone si configura come sistema di intelligenza artificiale (AI), si ripropone il problema, già evidenziato dalla dottrina, della mancanza di trasparenza in termini di funzionamento dell'algoritmo che governa il sistema di AI e che spesso comporta decisioni automatizzate[34]. Le modalità attraverso cui garantire il rispetto del principio di trasparenza nel trattamento dei dati personali e nell'impiego dell'AI è un tema che è stato ampiamento affrontato dalla dottrina costituzionalistica[35], per cui ci si limiterà a richiamare brevemente le principali declinazioni con cui il principio di trasparenza può trovare concreta attuazione anche nell'ambito dei droni nelle emergenze (quantomeno quelle di natura tecnica). Che il drone sia "solo" dotato di sensori e telecamere oppure si qualifichi anche come sistema di AI, il rispetto del principio di trasparenza si traduce innanzitutto nella garanzia di tracciabilità dei dati e dei procedimenti con cui viene raggiunta la decisione da parte del sistema di AI. Nel caso dei droni, ciò diventa particolarmente rilevante nel caso in cui essi siano dotati di tecnologie che permettono l'identificazione delle persone attraverso tecniche di riconoscimento facciale o identificazione biometrica[36]. Allo stesso modo, il principio trova ulteriore concretezza nel requisito di *explainability* delle decisioni assunte dal drone come sistema AI, che non si esaurisce nell'accesso ai codici dell'algoritmo ma si estende alla realizzazione di modelli di AI interpretabili o di strumenti che consentano di ottenere spiegazioni comprensibili, così da poter valutare le motivazioni che hanno portato alla decisione. Infine, esattamente come nella disciplina giuridica dell'AI e del trattamento dei dati personali, l'ultima dimensione in cui il principio di trasparenza potrebbe trovare una concreta attuazione è il livello di informazione sull'uso dei droni, così da garantire che gli individui coinvolti siano consapevoli delle modalità e le finalità con

31. Per una discussione più approfondita di questo punto, si rimanda a Vedaschi 2011.
32. Flaherty 2015.
33. Beduschi 2022.
34. Sul punto si rimanda in particolare a Fasan 2024.
35. Casonato 2020; Wachter 2018.
36. Cfr. Rostami-Farajollahi-Parvin 2024.

cui sono impiegati i droni e come vengono raccolti e trattati i dati.

In secondo luogo, la produzione di droni impiegati in ambito umanitario e civile è spesso caratterizzata da un partenariato pubblico-privato che solleva due ordini di problemi in termini di trasparenza[37]. Da un lato, il fatto che i droni (così come le ulteriori tecnologie di cui sono dotati) siano prodotti da enti privati comporta un'inevitabile asimmetria informativa, con il rischio che l'ente privato realizzi il proprio interesse invece dell'interesse pubblico[38]. A tal fine, è fondamentale che la produzione e fornitura di droni da parte di enti privati avvenga attraverso un sufficiente livello di trasparenza, così da garantire lo spazio per forme di controllo e tutelare i diritti individuali[39]. Dall'altro, è necessario aggiungere una considerazione etico-morale dovuta al fatto che, soprattutto all'inizio, molti dei droni utilizzati a scopo civile e umanitario erano frutto di un riutilizzo da un precedente uso militare, oppure erano essi stessi prodotti dalle stesse aziende che producevano anche droni militari. Questo è il caso dei droni italiani FALCO prodotti da Selex ES (Finmeccanica/Leonardo) e utilizzati, a scopo civile e umanitario, dalle Nazioni Unite nella missione di *peacekeeping* MONUSCO nella Repubblica Democratica del Congo[40] e più recentemente da Frontex nel Mediterraneo[41], mentre sono stati a lungo utilizzati a scopo militare in Pakistan[42] e ne è stata recentemente presentata una versione armata[43]. Allo stesso modo, i droni Global Hawk statunitensi furono largamente usati a scopo militare come droni di ricognizione nelle guerre in Iraq e in Afghanistan, e successivamente a scopo umanitario delle missioni di soccorso nelle zone colpite dal tifone Haiyan nelle Filippine[44]. In assenza di un'adeguata trasparenza sulla produzione dei droni, le organizzazioni umanitarie sarebbero esposte al rischio di violare i principi umanitari di indipendenza e neutralità che guidano l'operato delle organizzazioni nelle proprie missioni[45].

4. Droni e principio di eguaglianza

L'uso dei droni nelle emergenze mette a rischio anche un altro pilastro delle democrazie costituzionali, ossia il principio di eguaglianza. Ciò avviene sotto due profili principali, a seconda che il drone sia dotato o meno di tecnologie di intelligenza artificiale. Partendo dal caso in cui l'aeromobile a pilotaggio remoto sia dotato "solo" di telecamere, sensori e GPS, è opportuno ricordare l'uso dei droni per i c.d. *signature strikes* che ne aveva fatto l'amministrazione statunitense. Al contrario dei *targeted killings*, nei *signature strikes* gli obiettivi non sono individuati sulla base della loro identità, che rimane sconosciuta, ma del loro "comportamento" (*signature*), che li identifica come appartenenti a gruppi terroristi, come ad esempio la prossimità a campi di addestramento o il movimento di presunti combattenti al confine tra Pakistan e Afghanistan[46]. Come è facile immaginare, i *signature strikes* condotti durante la *war on terror* sono stati piuttosto controversi, non solo perché si tratta di una pratica potenzialmente in contrasto con il principio di distinzione su cui si fonda il diritto internazionale umanitario, ma anche perché l'individuazione dei *target* si basa fondamentalmente su approssimazioni e preconcetti sul "comportamento terrorista", dando origine a discriminazioni sulla base dell'etnia e dell'origine

37. De Londras 2022; Egger 2024.
38. Fidone 2016.
39. Reynaers–Grimmelikhuijsen 2015.
40. Karlsrud–Rosén 2018.
41. ENAC, Comunicato n. 86/2018 Sorveglianza marittima di Frontex con il drone falco EVO di Leonardo: supporto ENAC e rilascio certificazioni e autorizzazioni per operazioni.
42. Kweera 2023.
43. Gosselin-Malo 2023.
44. Emery 2016.
45. Cfr. Assemblea Generale dell'ONU, Risoluzione n. 46/182, 19 dicembre 1991, in particolare i punti 1 e 2 dell'Annex I "Guiding Principles".
46. Solis 2016, p. 560.

sociale[47]. Secondo tale ragionamento, il fatto che un individuo "si comporti come" (o "sembri") un terrorista pare sufficiente per confermare che questo lo sia realmente, al di là di qualsiasi distinzione tra combattenti e civili[48].

Se nel caso precedente, in assenza di AI, a compiere la discriminazione è l'essere umano che usa il drone per colpire indiscriminatamente, nel caso in cui i droni siano dotati di tecnologie di intelligenza artificiale tale discriminazione può avvenire attraverso l'AI stessa. Come già evidenziato dalla dottrina, i sistemi di AI possono presentare *bias* sviluppati in fase di programmazione e quindi generare effetti discriminatori sugli utenti[49], per esempio sulla base del genere, dell'orientamento sessuale o dell'etnia[50]. Ciò risulta ulteriormente problematico se tali *bias* informano le decisioni dei droni (o di chi li pilota da remoto), che attraverso la raccolta dei dati biometrici e le tecniche di riconoscimento facciale potrebbero per esempio identificare un soggetto come pericoloso in base alle sue caratteristiche fisiche o al proprio comportamento. Si pensi a uno scenario, non troppo ipotetico, in cui i droni vengono impiegati in operazioni di *law enforcement* o di sorveglianza durante una manifestazione e sulla base dei dati raccolti vengono effettuati degli arresti di cittadini appartenenti a minoranze[51], oppure ancora questi possono diventare veri e propri strumenti repressivi nelle democrazie illiberali o nei regimi autoritari[52]. Eppure, anche in questo caso è opportuno sottolineare la natura *dual-use* dei droni con tecniche di riconoscimento facciale. Infatti, tale tecnologia risulta fondamentale per individuare la presenza di esseri umani nelle missioni di ricerca e soccorso di dispersi in mare o di superstiti dopo un terremoto o un bombardamento[53]. Di nuovo, ciò che è essenziale è che tale tecnologia sia utilizzata in modo tale da evitare discriminazioni e preservare il principio di eguaglianza[54].

5. Droni e tutela dei diritti fondamentali

Come emerge in filigrana dalle pagine precedenti, l'uso dei droni nelle emergenze ha un impatto sostanziale anche sulla tutela dei diritti fondamentali, che deriva non solo dallo strumento utilizzato (cioè il drone), ma anche dall'eccezionalità della situazione di emergenza. Proprio per tale motivo, il contributo della dottrina costituzionalistica sugli stati di emergenza risulta di primaria importanza per comprendere al meglio la tensione tra la tutela dell'interesse generale e la limitazione di determinati diritti nelle emergenze. Le prossime pagine si concentreranno in particolare sul diritto alla vita, sul diritto al giusto processo e sul diritto alla privacy e la protezione dei dati personali. Tale scelta deriva dal fatto che questi sono i diritti maggiormente impattati dall'uso dei droni nelle emergenze, come anche dimostrato dai casi giurisprudenziali analizzati nel paragrafo 6.

5.1. Il diritto alla vita

È interessante notare come l'impatto dei droni nelle emergenze sul diritto alla vita sia duplice proprio in virtù della loro natura *dual-use*. Da un lato, l'uso dei droni a scopo umanitario ha il potenziale di espandere il diritto alla vita, contribuendo a salvare vite umane in condizioni in cui sarebbe molto difficile (o impossibile) farlo. Si pensi, di nuovo, ai droni utilizzati per identificare naufraghi, superstiti o dispersi che possono così ricevere un'adeguata assistenza medica, oppure ancora ai droni che consentono di distribuire medicinali salvavita e vaccini in zone isolate a causa di un disastro naturale o di un'epidemia. Dall'altro lato, al di fuori del contesto umanitario i droni possono

47. Sehrawat 2021, p. 70 ss.
48. Sul punto si rimanda in particolare a Heller 2013.
49. Zuiderveen Borgesius 2020; Heinrichs 2022.
50. Per approfondire tali aspetti si rimanda per esempio alla Parte IV dedicata ad "Artificial Intelligence and Non-Discrimination" in Quintavalla–Temperman 2023.
51. Sul punto si veda anche Mobilio 2021, p. 106 ss.; Menéndez González 2023.
52. Cfr. Katrak–Chakrabarty 2023.
53. Cfr. Rostami–Farajollani–Parvin 2022.
54. Sulla regolamentazione delle tecniche di riconoscimento facciale, si vedano Paolucci 2025; Menéndez González–Mobilio 2025.

essere determinanti anche per privare del diritto alla vita, per esempio attraverso le uccisioni mirate già richiamate in precedenza o attraverso gli attacchi dei droni armati nei conflitti. In tal senso, diventa fondamentale stabilire se tale privazione sia da considerare arbitraria o meno. Secondo il diritto internazionale dei conflitti armati, in tempo di guerra i belligeranti sono tenuti ad applicare sia le norme di diritto internazionale umanitario sia gli standard internazionali dei diritti dell'uomo[55], tranne che il belligerante non si avvalga delle clausole di deroga in caso di emergenza contenute in alcuni trattati internazionali o sovranazionali in materia di diritti dell'uomo[56].

Rispetto al diritto alla vita e al rapporto che intercorre tra diritto umanitario e diritti dell'uomo è utile richiamare la posizione della Corte internazionale di giustizia. Nel 1996, la Corte ha stabilito che la protezione derivante dal Patto sui diritti civili e politici non cessa in tempo di guerra, a meno che si invochi l'art. 4 secondo cui alcune norme possono essere derogate in caso di emergenza nazionale[57]. Al tempo stesso, la Corte ha aggiunto che il diritto alla vita sancito dall'art. 6(1) del Patto non rientra tra le norme cui è possibile derogare in virtù dell'art. 4, per cui il divieto di privazione arbitraria della vita è applicabile, in linea di principio, anche nei conflitti armati. In tal senso, il parametro per valutare la nozione di "privazione arbitraria" dev'essere il diritto dei conflitti armati, ossia la *lex specialis* applicabile in caso di guerra. In altre parole, per determinare una violazione o meno del diritto alla vita è necessario accertare se la privazione della vita è il risultato di un atto legittimo o illegittimo di belligeranza. Nel primo caso, non ci sarà una violazione in quanto la *lex specialis* (il diritto internazionale umanitario) prevale sulla *lex generalis* (i diritti dell'uomo). Nel caso in cui, invece, la privazione della vita avvenga attraverso un atto illegittimo, questa è considerata arbitraria ed è quindi illegittima anche in tempo di guerra.

Sempre in riferimento alla protezione del diritto alla vita e alle possibili deroghe in caso di guerra o di emergenza, è opportuno ricordare che l'art. 2 della CEDU è formulato in modo diverso dall'art. 6(1) del Patto. Infatti, l'art. 2 stabilisce non solo che il diritto alla vita è protetto dalla legge, ma anche una serie di eccezioni, tra cui la legittima difesa e l'uso della forza per eseguire un arresto o per reprimere una rivolta, purché sia conforme alla legge. Come noto, la Convenzione prevede anche una clausola di eccezione (art. 15), che in caso di guerra o emergenza nazionale permette alle parti contraenti di derogare ad alcuni diritti garantiti dalla Convenzione "nella stretta misura in cui la situazione lo richieda" (art. 15(1)), tranne alcuni diritti inderogabili. Tra questi ultimi rientra anche il diritto alla vita, cui non è possibile derogare "salvo il caso di decesso causato da legittimi atti di guerra" (art. 15(2)). Anche in questo caso, il parametro per valutare se l'atto di guerra sia legittimo o meno, e quindi determinare se ci sia stata o meno una violazione dell'art. 2 CEDU, è di nuovo il diritto internazionale umanitario[58]. Dal quadro appena delineato, è quindi evidente come sia fondamentale determinare se l'uso del drone che porta alla privazione del diritto alla vita avvenga o meno nell'ambito di applicazione del diritto internazionale dei conflitti armati, poiché in caso contrario prevarrebbero i diritti dell'uomo e quindi l'atto costituirebbe un'esecuzione extragiudiziale[59].

5.2. Il diritto al giusto processo

Nel medesimo contesto che potrebbe portare alla privazione arbitraria del diritto alla vita, ossia quello dei *targeted killings* a mezzo drone, si inserisce anche la necessità di garantire il diritto al giusto processo. Infatti, uno degli elementi che compone la giustificazione della pratica degli omicidi mirati statunitensi si basa sull'impossibilità di catturare, arrestare e processare l'individuo identificato come *target* per i propri crimini[60]. Tuttavia,

55. Ronzitti 2021, p. 175.
56. Si fa riferimento, in particolare, all'art. 4 del Patto internazionale sui diritti civili e politici e all'art. 15 della Convenzione europea dei diritti dell'uomo.
57. ICJ, *Reports 1996*, p. 240, par. 25.
58. Ronzitti 2021, p. 177.
59. Cfr. Flaherty 2015, p. 27; Vedaschi 2011, p. 1225.
60. Solis 2016, p. 554 ss.

la vicenda processuale di Abu Ghaith, genero di Osama bin Laden e uno dei principali esponenti di al-Qaeda coinvolti negli attacchi dell'11 settembre, dimostra che strade alternative agli omicidi mirati erano percorribili. Dopo essere stato arrestato in Turchia nel 2013 da degli ufficiali giordani, Ghaith è stato processato e condannato da un tribunale statunitense nel marzo del 2015[61]. Tuttavia, le maggiori critiche sulla dubbia compatibilità degli omicidi mirati a mezzo drone con il principio del *due process* sono state sollevate dall'uccisione di cittadini statunitensi considerati parte di organizzazioni terroristiche, come nel caso di Anwar al-Awlaki, presunto leader di un'organizzazione associata ad al-Qaeda ucciso da un drone nel 2011. Nel giugno 2014, in seguito a una richiesta sulla base del *Freedom of Information Act* da parte dell'ACLU, la Corte d'Appello del Secondo Circuito ha ordinato il rilascio di un memorandum dell'Office of Legal Counsel (OLC), solo parzialmente censurato, che contenesse la base giuridica per l'omicidio del cittadino statunitense al-Awlaki[62].

Al di là delle specifiche giustificazioni avanzate dal governo[63], è interessante soffermarsi brevemente su una questione riguardante il dibattito sul *due process* nei casi di omicidi mirati a mezzo drone, legato all'applicazione extraterritoriale del *due process*[64]. Infatti, se da un lato la giurisprudenza della Corte Suprema ha stabilito già da tempo che i cittadini statunitensi sono protetti dai diritti garantiti nella Costituzione anche al di fuori dei propri confini, dall'altro lato è meno consolidata l'interpretazione dell'applicazione extraterritoriale dei diritti costituzionali ai non-cittadini[65]. In passato, la Corte si è espressa sul tema in altre circostanze, in particolare nei casi di detenzione a Guantanamo[66], ma mai nei casi di *targeting*, motivo per cui l'uccisione di al-Awlaki è stata particolarmente rilevante nel dibattito statunitense. In particolare, parte della dottrina si è interrogata su come i tre fattori del "Mathews test"[67] elaborato dalla Corte Suprema possano essere applicati ai casi di *targeting*[68]. Come già emerso nelle pagine precedenti e come si elaborerà maggiormente in seguito, anche in questo caso si ripresenta la difficoltà di valutare il rischio di una "*erroneous deprivation of life*", a cui si aggiunge la necessità di considerare eventuali ulteriori garanzie procedurali per evitare abusi di potere[69].

61. Flaherty 2015, p. 22.
62. Questo e altri documenti sui *targeted killings* statunitensi resi pubblici sono stati raccolti da Jaffer 2016. La pubblicazione di tali documenti è avvenuta sia attraverso decisioni di corti distrettuali sia attraverso le richieste avanzate in base al *Freedom of Information Act*, la legge statunitense che prevede l'obbligo di divulgazione totale o parziale di informazioni precedentemente non pubblicate dal governo statunitense, qualora ne ricevesse richiesta.
63. Secondo i documenti pubblicati tra il 2010 e il 2014, il fatto che al-Awlaki fosse stato individuato come leader di un'organizzazione vicina ad al-Qaeda era sufficiente per identificarlo come *target*. Tale posizione è stata ampiamente discussa dalla dottrina, evidenziando come l'avvento del terrorismo internazionale abbia pericolosamente riscritto le condizioni per l'esistenza di un conflitto armato, con il rischio di giustificare l'uso della forza al di fuori dei propri confini statali (con o senza il consenso dello Stato terzo in cui si compie il *targeted killing*). Per un'analisi critica sul punto e della compatibilità dei *targeted killing* con lo *jus ad bellum* e lo *jus in bello*, si rimanda a Vedaschi 2011; Brooks 2014; Flaherty 2015, pp. 27-33; Ronzitti 2021, p. 332; Sassoli 2024, pp. 554-556.
64. Cfr. Pearlstein 2013.
65. Per una posizione fortemente a favore dell'estensione della protezione del *due process* ai non-cittadini, si rimanda a Flaherty 2015, pp. 34-37.
66. Si veda in particolare *Boumediene v. Bush*, 553 U.S. 723 (2008).
67. In *Mathews v. Eldridge*, 424 U.S. 319 (1976), la Corte Suprema degli Stati Uniti ha cristallizzato i criteri necessari per valutare il bilanciamento tra gli interessi nei casi di privazione della proprietà (cfr. Mashaw 1976).
68. Il Mathews test era già stato applicato dalla Corte Suprema in *Hamdi v. Rumsfled* (524 U.S. 507 (2004)) per determinare quale forma di protezione del *due process* potesse essere riconosciuta al ricorrente, un cittadino statunitense detenuto per il suo presunto coinvolgimento con gruppi talebani in Afghanistan.
69. Per un'analisi approfondita si rimanda a Pearlstein 2013, p. 6 ss. e Flaherty 2015, pp. 38-39, 42.

5.3. Il diritto alla privacy e la protezione dei dati personali

L'impiego dei droni nelle emergenze comporta notevoli rischi anche per la tutela del diritto alla privacy e la protezione dei dati personali[70]. Il quadro è particolarmente critico soprattutto nei casi in cui i droni sono utilizzati dalle forze dell'ordine o nelle operazioni di contrasto al terrorismo[71], in quanto non rientrano nell'ambito di applicazione del Regolamento UE 2016/679 relativo alla protezione dei dati personali[72]. Ciò implica che la regolamentazione sia lasciata ai singoli Stati, creando potenziali divergenze in termini di standard di protezione e tutele e lasciando che le norme a tutela della privacy siano generalmente erose a vantaggio di quelle a tutela della sicurezza pubblica[73].

Un ambito particolarmente interessante e ancora poco esplorato è quello umanitario, in cui i rischi per la privacy e la protezione dei dati personali derivanti dall'uso dei droni sono stati affrontati nell'*ICRC Handbook on Data Protection*[74]. Il testo riconosce come le tecnologie avanzate integrate nei droni umanitari consentano la raccolta di diverse tipologie di dati (visuali, multispettrali, termici) che possono condurre al riconoscimento diretto o indiretto degli individui attraverso sistemi di riconoscimento facciale o lettura di microchip usati nei passaporti per l'identificazione a radiofrequenza (RFID). Una delle principali criticità che si verifica nelle emergenze (umanitarie e non solo) riguarda l'impossibilità di ottenere un consenso informato. L'*ICRC Handbook* sostiene che le condizioni emergenziali e la natura delle zone d'intervento rendono irrealistico considerare il consenso come base legittima per il trattamento dei dati personali e osserva che la libertà del consenso risulta compromessa quando i soggetti si trovano in situazioni di pericolo e necessitano di assistenza umanitaria[75]. Per affrontare questa problematica, l'Ufficio delle Nazioni Unite per gli Affari Umanitari ha proposto nel 2014 un approccio basato sull'informazione preventiva alle comunità e autorità locali riguardo ai dettagli operativi e agli obiettivi delle missioni, così da ottenere un "consenso informato" da parte degli individui coinvolti[76]. L'*Handbook* ha successivamente sviluppato il concetto di "consenso di comunità" o "consenso delle autorità" come alternativa al consenso individuale, pur riconoscendo le criticità giuridiche di tale approccio. Infatti, questo potrebbe comportare la creazione di nuovi spazi di discriminazione e marginalizzazione, dando per scontato che l'individuo si senta necessariamente rappresentato dal proprio "gruppo". Secondo le linee guida del Comitato Internazionale della Croce Rossa, in assenza di consenso individuale, le organizzazioni umanitarie possono procedere alla raccolta e al trattamento dei dati personali basandosi sull'interesse legittimo dell'organizzazione e sull'interesse vitale dell'interessato[77]. Questo principio consente di bilanciare la mancanza del consenso con altri diritti fondamentali quali il diritto alla vita, all'integrità personale, alla sicurezza e alla dignità umana. L'ICRC riconosce che, in circostanze particolarmente critiche, la presenza di un interesse vitale può essere anche presunta, purché sia dimostrata o quantomeno sia probabile il contributo apportato dai droni alla protezione di interessi privati superiori come la vita, l'integrità e la sicurezza. Il rispetto della privacy richiede che i dati personali vengano trattati solo se "adeguati, pertinenti e non eccedenti in relazione alle finalità per cui sono stati

70. Cfr. Finn–Wright 2016; Merla 2016; Takahashi 2012.
71. Sul punto si veda per esempio Marin 2017.
72. Regolamento UE 2016/679 – Art. 1(2), lett. d: "[Il presente regolamento non si applica ai trattamenti di dati personali] effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse".
73. Losano 2018, p. 36.
74. Kuner–Marelli 2020, p. 111 ss.
75. *Ivi*, p. 115.
76. UNOCHA 2014, p. 10.
77. Kuner–Marelli 2020, p. 116.

raccolti"[78]. A tal fine, le organizzazioni umanitarie devono effettuare valutazioni rigorose sulla necessità e proporzionalità del trattamento, adottando tecnologie proporzionate e misure di protezione conformi ai principi di *privacy-by-design* e *privacy-by-default*[79], nel rispetto del principio di minimizzazione dei dati.

6. Droni e forme di controllo

L'uso dei droni nelle emergenze solleva alcune criticità in termini di *accountability* dell'esecutivo, specialmente nei contesti in cui i droni sono utilizzati nelle emergenze politiche. Di seguito si prenderanno in esame due utilizzi specifici dei droni che sono stati oggetto di controllo giurisdizionale, ossia i droni per gli omicidi mirati nei contesti di conflitto e i droni di sorveglianza utilizzati da parte delle forze dell'ordine o governative.

6.1. I droni per gli omicidi mirati

Il caso dei *targeted killings*, soprattutto se rivolti a cittadini statunitensi, ha generato un ampio dibattito negli Stati Uniti su quali forme di controllo siano più appropriate per valutare la costituzionalità degli attacchi a mezzo drone. Infatti, alcuni hanno suggerito forme di controllo giurisdizionale *ex-post*[80], altri hanno sottolineato la necessità di prevedere anche un controllo giurisdizionale *ex-ante*[81], altri ancora hanno proposto una forma più rigorosa di controllo interno all'esecutivo[82]. Come facilmente immaginabile, si tratta di una questione di non facile risoluzione in quanto le possibili opzioni presentano diversi profili di criticità[83]. Infatti, affidare il controllo ad organi interni all'esecutivo o a commissioni facenti capo ai servizi di *intelligence* parrebbe particolarmente critico sotto il profilo dell'indipendenza del giudizio, così come l'individuazione di organi *ad hoc* solleverebbe diversi problemi relativamente alla loro composizione e alla relativa posizione all'interno del sistema giudiziario o amministrativo. Eppure, per quanto l'affidamento di una forma di controllo a un organo giudiziario consentirebbe ampie garanzie di indipendenza, ci si potrebbe comunque interrogare sull'appropriatezza di tale organo per il tipo di verifica richiesta.

Il tema della *justiciability* della pratica dei *targedet killings* era già emerso in due sentenze, una resa dalla Corte Suprema israeliana, l'altra dalla Corte Distrettuale per il Distretto della Columbia, chiamate a valutare la legittimità della pratica in sé (al di là dell'impiego o meno di droni). Da un lato, la Corte israeliana aveva ritenuto che la scelta di ricorrere agli omicidi mirati rientrasse negli ambiti soggetti al controllo giurisdizionale e non fosse una questione unicamente politica[84]. Il giudice Barak, in particolare, aveva sostenuto la giustiziabilità del caso sia sotto il profilo normativo, riconoscendo l'esistenza di una norma giuridica alla base della decisione, sia sotto il profilo istituzionale, in

78. *Ivi*, p. 120 [traduzione dell'autrice].

79. Cfr. Rubinstein 2011; Willis 2014.

80. Sul punto si rimanda alla proposta di Vladeck, secondo cui una possibile soluzione potrebbe essere un'espansione della giurisdizione della *Foreign Intelligence Surveillance Court* (FISC) ai casi di *targeted killings*, oppure il suo utilizzo come modello per istituire una corte *ad hoc* per giudicare tali questioni (Vladeck 2014).

81. Si veda in particolare la posizione di Flaherty, il quale richiama il Mathews test per sostenere la necessità di un controllo preventivo e non (solo) successivo (Flaherty 2015). Tale necessità è sostenuta anche da Cassese, secondo cui la presenza di meccanismi di monitoraggio sia *ex-ante* sia *ex-post* darebbe piena attuazione allo spirito e alle richieste del diritto internazionale umanitario (Cassese 2006).

82. Questa è, per esempio, l'approccio adottato da Gonzales, secondo cui è necessario adottare ulteriori controlli interni all'esecutivo secondo il modello dei *Combat Status Review Tribunals* (CSRTs), istituiti originariamente per decidere sui casi di detenzione degli *unlawful enemy combatants*. Secondo Gonzales, un organo basato sull'esperienza dei CSRTs consentirebbe di dotarsi di un arbitro formale e neutrale nel processo di approvazione dei *targeted killings* (Gonzales 2013).

83. Sul punto si veda anche quanto osservato da Vedaschi 2011, p. 1227.

84. Corte Suprema di Israele, *Public Committee against Torture in Israel v. Government of Israel*, HCJ 769/02, 13 dicembre 2006. Per alcuni commenti, più o meno critici, si rimanda in particolare a Benvenuti 2007; Cassese 2006; Eichensehr 2007.

quanto esso riguardava un diritto umano imprescindibile come il diritto alla vita e l'uccisione di civili innocenti[85]. Dall'altro lato, la Corte Distrettuale statunitense ha mostrato un comportamento più oscillante sulla giustiziabilità o meno dei *targeted killings*, anche nei casi in cui i *target* fossero cittadini statunitensi. Infatti, in *Al-Aulaqi v. Obama*[86], la Corte aveva rigettato la richiesta dei ricorrenti di verificare la legittimità della decisione del Presidente di autorizzare l'omicidio mirato nei confronti di un cittadino statunitense senza alcun *due process*, abbracciando quindi la prospettiva della non-giustiziabilità (*non-justiciability*) dei *targeted killings* in virtù della loro natura prettamente politica. Alcuni anni dopo, in *Al-Aulaqi v. Panetta*[87], la Corte si è trovata davanti a un caso simile, in cui era chiamata a esprimersi sulla responsabilità degli ufficiali statunitensi per la morte di un cittadino statunitense ucciso da un attacco di un drone in Yemen. Discostandosi dalla precedente decisione, la Corte si è rifiutata di applicare la dottrina della non-giustiziabilità e ha criticato aspramente il governo statunitense per la mancata cooperazione nel fornire le informazioni richieste. Nella sua decisione, la Corte Distrettuale ha sottolineato come il potere di dichiarare guerra e di garantire la sicurezza nazionale non conferiva al Presidente e al Congresso "carta bianca" nel privare i cittadini statunitensi del diritto alla vita, senza *due process* e *judicial review*[88]. Per quanto l'esito della decisione sia stato deludente per i ricorrenti, il fatto che una corte statunitense non si sia sottratta dal valutare il caso è comunque un risultato significativo, che ha aperto una strada verso un maggiore controllo sul processo decisionale del potere esecutivo percorribile anche in futuro[89].

6.2. I droni di sorveglianza

Un altro ambito in cui alcune corti si sono espresse, ben più recentemente, riguarda l'uso dei droni nelle operazioni di sorveglianza da parte delle forze dell'ordine o governative. Sempre negli Stati Uniti, i droni sono ampiamente impiegati sia dalle agenzie di sicurezza pubblica statali e locali sia dalle forze dell'ordine per cercare e identificare sospetti criminali e monitorare spazi pubblici[90]. L'uso sempre più capillare dei droni di sorveglianza da parte di soggetti governativi ha sollevato anche notevoli critiche, soprattutto relativamente al rispetto della privacy. In passato, la Corte Suprema aveva posto il Quarto Emendamento come limite all'uso delle "nuove" tecnologie negli spazi pubblici, come nel caso delle intercettazioni telefoniche o ambientali[91]. In particolare, in *Katz v. United States*[92], la Corte aveva affermato che l'uso della tecnologia da parte delle forze dell'ordine costituiva una violazione del Quarto Emendamento, non solo perché era "an intrusion into a constitutionally protected area"[93], ma anche perché le ricerche effettuate erano contrarie a una ragionevole "expectation of privacy"[94] da parte del ricorrente. Tuttavia, la successiva giurisprudenza della Corte non ha applicato il *reasonable expectation of privacy test* in modo espansivo, sostenendo che molte delle attività svolte nello spazio pubblico non sono protette dall'ambito di sorveglianza governativa[95]. Solo in

85. Corte Suprema di Israele, *Public Committee against Torture in Israel v. Government of Israel*, par. 49-54. Per un'analisi della *normative and institutional justiciability*, si rimanda a Cassese 2006, p. 340 ss.
86. *Al-Aulaqi v. Obama*, 727 F. Supp. 2d 1 (D.D.C. 2010).
87. *Al-Aulaqi v. Panetta*, 35 F. Supp. 3d 56 (D.D.C. 2014).
88. *Al-Aulaqi v. Panetta*, parr. 20-21.
89. Sul ruolo delle corti nazionali nei conflitti, si segnala Weill 2014; Weill 2016.
90. Sull'uso dei droni e di altre tecnologie, tra cui tecniche di riconoscimento facciale e televisione a circuito chiuso (CCTV), e le relative implicazioni sui diritti, si segnala Weaver 2021, mentre sull'uso da parte delle forze dell'ordine negli Stati Uniti si rimanda a Finklea 2023.
91. Cfr. *Olmstead v. United States*, 316 U.S. 129 (1928); *Goldman v. United States*, 277 U.S. 438 (1942).
92. *Katz v. United States*, 389 U.S. 347 (1967).
93. *Ivi*, p. 353.
94. *Ivi*, pp. 351-352.
95. Cfr. Weaver 2021, p. 60 ss.

Carpenter v. United States[96], la Corte Suprema ha riconosciuto una violazione del Quarto Emendamento in un caso relativo all'uso dei dati di tracciamento da parte della polizia per verificare gli spostamenti di un sospettato. Secondo la Corte, da quei dati era possibile risalire a informazioni riguardanti la sfera privata del ricorrente al di là dei suoi movimenti, ma anche i suoi legami familiari, affettivi, professionali e religiosi[97]. In altri casi, la Corte ha infatti confermato una violazione del Quarto Emendamento quando le attività di sorveglianza da parte di soggetti governativi andavano a invadere la sfera privata degli individui[98].

Per quanto riguarda nello specifico i droni di sorveglianza, negli ultimi anni alcune corti si sono confrontate con l'uso di tale tecnologia da parte delle forze governative. In *Long Lake Township v. Maxon*[99], la municipalità aveva utilizzato un drone per sorvolare la proprietà del ricorrente e raccogliere delle prove fotografiche per sostenere la presunta violazione di alcune norme di zonizzazione[100]. Il ricorrente aveva quindi impugnato la decisione della municipalità lamentando una violazione del Quarto Emendamento e sostenendo che le prove raccolte non potessero essere utilizzate poiché raccolte in modo illegittimo. La corte di prima istanza aveva rigettato la richiesta di Maxon, concludendo che l'uso del drone non costituisse una perquisizione irragionevole[101]. La decisione è stata poi rovesciata dalla Corte d'Appello, facendo nuovamente riferimento alla *reasonable expectation of privacy* già formulata dalla Corte Suprema[102]. La decisione della Corte d'Appello è particolarmente significativa perché è il primo caso in cui si riconosce esplicitamente la differenza qualitativa che intercorre tra il moderno drone di sorveglianza e i precedenti mezzi di perlustrazione aerea ritenuti compatibili con il Quarto Emendamento, introducendo il requisito di un mandato per poter utilizzare i droni di sorveglianza. Così facendo, le prove raccolte dalla municipalità non potevano essere utilizzate. Il caso è giunto davanti la Corte Suprema del Michigan nel 2022, la quale ha spostato l'attenzione dalla violazione del Quarto Emendamento attraverso l'uso del drone all'applicabilità della regola di esclusione (*exclusionary rule*) riguardo l'utilizzo delle prove fotografiche raccolte dal drone. Riconoscendo la non applicabilità dell'*exclusionary rule*, la Corte si è sottratta dal valutare se l'uso del drone per la perlustrazione aerea costituisce una perquisizione irragionevole, perdendo così un'occasione importante per riaffermare il diritto alla privacy alla luce delle nuove tecniche di sorveglianza[103].

Se nei primi casi analizzati sui *targeted killings* il tema riguardava la giustiziabilità o meno di questioni intimamente politiche, nel caso dei droni di sorveglianza emerge un'altra difficoltà riscontrata dalle corti, ossia il necessario bilanciamento tra la sicurezza pubblica e la tutela dei diritti individuali[104]. In tal senso è importante richiamare una sentenza del *Conseil d'État* francese, che nel 2020 ha accolto la richiesta di due associazioni di interrompere il programma di sorveglianza aerea a mezzo drone predisposto dal prefetto della polizia di Parigi durante l'emergenza sanitaria. Nello specifico, i droni erano impiegati dalla polizia per verificare il rispetto delle misure di contenimento del virus, anche dopo l'allentamento di tali misure[105]. Le associazioni sostenevano che l'uso di

96. *Carpenter v. United States*, 585 U.S. 296 (2018).
97. Come già sostenuto dalla giudice Sotomayor nella sua opinione concorrente in *United States v. Jones*, 565 U.S. 400, 415 (2012).
98. Cfr. *United States v. Karo*, 486 U.S. 705 (1984); *Kyllo v. United States,* 533 U.S. 27 (2001).
99. *Long Lake Township v. Maxon*, 15 N.W.3d 118 (Mich. 2024).
100. Per un'analisi approfondita del caso, si rimanda a Khalil 2023; Massa 2025 e il commento pubblicato sulla Harvard Law Review.
101. *Long Lake Township v. Maxon*, No. 18-34553-CE (Mich. Cir. Ct., 2 May 2019).
102. *Long Lake Township v. Maxon*, 970 N.W.2d 893, 899 (Mich. Ct. App. 2021).
103. *Long Lake Township v. Maxon*, 15 N.W.3d 118, 120 (Mich. 2024).
104. Weaver 2021, p. 64.
105. Conseil d'État, *Association La Quadrature Du Net et la Ligue de Droits de l'Homme*, nos. 440442, 440445, 18 mai 2020 (ECLI:FR:CEORD:2020:440442.20200518).

droni che sorvolano lo spazio pubblico al di fuori di qualsiasi quadro di regolamentazione, associato a dispositivi per l'acquisizione di immagini, costituisse un trattamento dei dati personali illegittimo e una violazione del diritto alla vita privata e familiare e del diritto alla tutela dei dati personali. Pur riconoscendo le legittime finalità dell'uso dei droni, dettate dalla necessità di preservare la sicurezza pubblica, il *Conseil* ha affermato che il drone di sorveglianza rientra nell'ambito di applicazione della Direttiva UE 2016/680 del 27 aprile 2016 (c.d. *Law Enforcement Directive*)[106], la quale all'art. 1(1) stabilisce "le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, *incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica*"[107].

Richiamando tale Direttiva, il *Conseil* osserva che le tecnologie di cui sono dotati i droni permettono la raccolta di dati identificativi e non dispongono di alcun dispositivo tecnico atto a impedire che le informazioni raccolte possano condurre a fini diversi da quelli originariamente perseguiti. Pertanto, secondo il Consiglio di Stato, in tali circostanze i dati che potrebbero essere raccolti devono essere considerati di carattere personale[108]. Tenuto conto dei rischi di un utilizzo dei dati personali contrario alla normativa, il *Conseil* conclude che l'attuazione di tale trattamento di dati personali, per conto dello Stato, senza il previo intervento di un testo normativo che ne autorizzi la creazione e ne stabilisca le modalità di utilizzo da rispettare obbligatoriamente, così come le adeguate garanzie, costituisce una grave e manifestatamente illegale violazione del diritto al rispetto della vita privata e familiare[109]. Pertanto, con questa decisione, il *Conseil* francese ha ordinato la cessazione del programma di droni di sorveglianza fino a quando la violazione individuata sarà sanata mediante l'intervento del legislatore[110]. Al parlamento francese, in particolare, è stato richiesto di introdurre l'obbligo di creare un trattamento che rispetti la Direttiva UE 2016/680, dotando i droni di dispositivi tecnici tali da rendere impossibile, indipendentemente dall'uso che ne viene fatto, l'identificazione delle persone filmate[111].

Una posizione simile è stata adottata dal *Conseil constitutionnel* nel 2021[112] relativamente all'uso dei droni di sorveglianza da parte delle forze dell'ordine, questa volta non solo in contesti di emergenza ma anche in materia di polizia giudiziaria e amministrativa. In questo caso, il *Conseil constitutionnel* ha dichiarato parzialmente incostituzionale la *Loi pour une sécurité globale préservant les libertés*[113], tra cui l'art. 47 sul trattamento dei dati raccolti dai droni. Nella sua decisione, il *Conseil* ha osservato come i droni possano essere utilizzati dalle forze dell'ordine statali e locali per un'ampia varietà di operazioni, che includono l'esecuzione di sanzioni penali e il mantenimento della sicurezza e dell'ordine pubblico. È interessante notare come nella decisione siano menzionati esplicitamente anche determinati contesti di emergenza politica, tra cui spicca la prevenzione di atti terroristici. Allo stesso modo, si riconosce che le caratteristiche tecniche dei droni permettono di catturare immagini di un elevato numero di persone e di seguirne gli spostamenti in un ampio perimetro. Alla luce di ciò, il *Conseil constitutionnel* ha stabilito che l'attuazione di tali sistemi di sorveglianza, così come previsto dalla legge, non era accompagnata da adeguate garanzie atte a salvaguardare il diritto al rispetto della vita privata e familiare. In particolare, il Consiglio costituzionale ha rilevato che il legislatore francese non ha fissato alcun limite massimo alla durata dell'autorizzazione a ricorrere ai droni di

106. *Association La Quadrature Du Net*, parr. 13-15.
107. Direttiva UE 2016/680, art. 1(1), corsivo aggiunto.
108. *Association La Quadrature Du Net*, par. 16.
109. *Ivi*, par. 18.
110. *Ivi*, par. 19.
111. *Ibidem.*
112. Décision du Conseil constitutionnel n° 2021-817 DC du 20 mai 2021.
113. *Loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés.*

sorveglianza, né alcun limite al perimetro in cui può essere attuata tale sorveglianza[114]. Per questi motivi, il *Conseil* ha ritenuto che il legislatore non abbia garantito un adeguato equilibrio tra gli obiettivi di valore costituzionale di prevenzione delle violazioni dell'ordine pubblico e il diritto al rispetto della vita privata[115].

Appena un anno dopo, il *Conseil constitutionnel* si è espresso nuovamente sull'uso dei droni di sorveglianza[116], questa volta relativamente alla costituzionalità della *Loi relative à la responsabilité pénale et à la sécurité intérieure*[117], con specifico riferimento all'uso dei droni di sorveglianza previsto dall'art. 15. Per quanto anche in questo caso la legge non riguardi esclusivamente i contesti emergenziali, è comunque utile tenere conto di questa decisione poiché il *Conseil* ha cambiato orientamento e ha ritenuto che le disposizioni riguardanti i droni non fossero in violazione della Costituzione, seppur con alcune riserve interpretative[118]. L'unica eccezione è costituita dall'ottavo comma dell'art. 15, relativo all'uso dei droni da parte della polizia municipale, dichiarato incostituzionale e perciò censurato[119]. Secondo il *Conseil*, infatti, in questo caso il legislatore non è stato in grado di garantire un adeguato equilibrio tra requisiti costituzionali come nel caso dei droni utilizzati dalle forze dell'ordine statali. In riferimento alla medesima legge, si è pronunciato anche il *Conseil d'État* nel 2023, confermando la conformità delle disposizioni con il quadro giuridico francese e con la normativa europea in materia di privacy e dati personali[120]. Nonostante la richiesta dei ricorrenti di sospendere la legge sia stata rigettata, è interessante notare come il Consiglio di Stato abbia sottolineato che l'autorizzazione da parte del prefetto a utilizzare i droni di sorveglianza possa essere sempre soggetta al controllo giurisdizionale per verificarne la legittimità[121].

Per quanto la decisione del *Conseil d'État* del 2020 sui droni di sorveglianza sia stata poi superata dalle successive decisioni del *Conseil constitutionnel* nel 2022 e dello stesso *Conseil d'État* nel 2023, essa è ugualmente significativa poiché si tratta di un caso, riguardante nello specifico l'uso dei droni in un contesto emergenziale (l'emergenza sanitaria), in cui un organo giudiziario non si è sottratto dal valutarne la compatibilità con la tutela dei diritti fondamentali. Tale decisione evidenzia come le corti, poste davanti al caso concreto, possano svolgere un ruolo determinante nel bilanciare la necessità di preservare la sicurezza pubblica dettata dall'emergenza con la tutela dei diritti fondamentali, chiamando il legislatore a intervenire per colmare eventuali lacune. Al contrario della Corte Suprema del Michigan, che ha evitato di esprimersi sul rispetto del Quarto Emendamento, il *Conseil* ha quindi potenzialmente aperto la strada a un uso dei droni nelle emergenze che risponda prima di tutto alla tutela dei diritti fondamentali e alla legge, svolgendo un'importante forma di controllo su tale uso e altrettante forme di rimedio in caso di violazioni[122].

7. Riflessioni conclusive

L'analisi svolta nel presente articolo evidenzia l'ampio spettro di sfide per il costituzionalismo generate dall'uso dei droni, mettendo in discussione

114. Conseil constitutionnel, 2021-817 DC, parr. 138-140.
115. Conseil constitutionnel, 2021-817 DC, par. 141.
116. Décision du Conseil constitutionnel n° 2021-834 DC du 20 janvier 2022.
117. *Loi n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure.*
118. Conseil constitutionnel, 2021-834 DC, parr. 27-30.
119. Conseil constitutionnel, 2021-834 DC, parr. 34-38.
120. Conseil d'État, *La Ligue de Droits de l'Homme*, et al., no. 473547, 24 mai 2023 (ECLI:FR:CEORD:2023:473547.20230524).
121. Per un'analisi più approfondita, si rimanda al commento *French Conseil d'État authorises the use of drones by law enforcement agencies* pubblicato in ai-regulation.com.
122. In tal senso è utile richiamare quanto già elaborato dalla dottrina giuspubblicistica rispetto agli stati di emergenza. Questa posizione richiama infatti la c.d. "teoria monista" sul principio di necessità, secondo cui i poteri di emergenza dettati dalla necessità sono comunque poteri derivati dal potere costituente originario e incontra dei limiti e dei vincoli stabiliti dall'ordine giuridico preesistente. Per un'analisi più completa, si veda Piergigli 2023-a, p. 606.

pilastri come il principio di trasparenza nei processi decisionali, il divieto di discriminazione, la tutela dei diritti fondamentali e la garanzia di adeguate forme di controllo (politico e/o giurisdizionale). In quanto tali, esse richiedono un quadro giuridico capace di regolare organicamente l'uso dei droni al fine di riconciliare la necessità di preservare la sicurezza pubblica con i principi del costituzionalismo.

Attualmente, il quadro di regolamentazione si presenta frammentato tra normative internazionali, sovranazionali e statali ed è ulteriormente complicato dal fatto che, come detto, i droni si qualificano come tecnologie *dual-use*. Infatti, i droni utilizzati a scopo militare nei conflitti armati rientrano nell'ambito del diritto internazionale umanitario[123], in particolare nella disciplina della guerra aerea[124] e delle "nuove armi"[125]. Per quanto riguarda, invece, i droni impiegati a scopo civile, la regolamentazione si è articolata a livello internazionale, grazie all'operato dell'*International Agency for Civil Aviation* (ICAO) delle Nazioni Unite[126], oltre che a livello nazionale e sovranazionale, con l'adozione di diverse normative statali[127] e del Regolamento UE 2019/947 sull'utilizzo di aeromobili a pilotaggio remoto[128]. Inoltre, il quadro di regolamentazione dei droni nelle emergenze si estende ulteriormente se i droni si configurano come sistemi di AI[129]. In quel caso, si deve fare riferimento anche alle normative che disciplinano l'intelligenza artificiale, con le conseguenti differenze tra gli approcci adottati finora[130]. Nel contesto europeo, lo studio dell'uso dei droni nelle emergenze, quantomeno di natura tecnica, diventa essenziale se si considera che questi potrebbero facilmente rientrare nelle categorie di sistemi ad alto rischio previste dall'*Artificial Intelligence Act*, specialmente nel caso in cui i droni siano dotati di tecniche per il riconoscimento facciale e l'identificazione biometrica o siano utilizzati per il controllo dei confini[131].

È quindi evidente che la regolamentazione dei droni nelle emergenze al fine di preservare l'ordine pubblico (e la sicurezza) nel rispetto dei principi del costituzionalismo non sia un nodo facile da sciogliere e richieda un approccio di governance "costituzionalmente orientata" fondata su strumenti normativi flessibili e capaci di adattare le

123. In termini generali, la dottrina sembra concordare nel considerare il diritto umanitario abbastanza flessibile da adattarsi allo sviluppo tecnologico e nell'osservare che qualsiasi restrizione all'uso di determinate tecnologie deve tenere necessariamente conto del fatto che le stesse potrebbero avere importanti effetti benefici se applicati in campo civile e umanitario (cfr. Liivoja–Leins–McCormack 2016, p. 622; Kreps–Maxey 2021, p. 83 ss.; Nasu–McLaughlin 2014; Schulzke 2025).

124. Ronzitti 2019.

125. Art. 36 "Nuove armi" – I Protocollo Aggiuntivo alle Convenzioni di Ginevra del 12 agosto 1949 relativo alla Protezione delle Vittime dei Conflitti Armati Internazionali: "Nello studio, messa a punto, acquisizione o adozione di una nuova arma, di nuovi mezzi o metodi di guerra, un'Alta Parte contraente ha l'obbligo di stabilire se il suo impiego non sia vietato, in talune circostanze o in qualunque circostanza, dalle disposizioni del presente Protocollo o da qualsiasi altra regola del diritto internazionale applicabile a detta Alta Parte contraente". Per un'analisi più approfondita, si veda International Committee of the Red Cross 2006, mentre sulla disciplina dei sistemi d'arma autonomi, in cui rientrano alcuni droni armati, si rimanda al contributo di Amoroso in questa sezione monografica (Amoroso 2025).

126. In particolare, l'ICAO ha recentemente pubblicato delle linee guida per l'utilizzo dei droni nelle missioni umanitarie o nelle risposte alle emergenze, così da fornire un quadro comune agli Stati membri della Convenzione di Chicago (*Unmanned Aircraft Systems (UAS) for Humanitarian Aid and Emergency Response Guidance*, April 2025).

127. Per le normative statali sui droni, si segnala, online, il *Global Drone Regulation Database*.

128. Regolamento UE 2019/947 relativo a norme e procedure per l'esercizio di aeromobili senza equipaggio del 24 maggio 2019.

129. Cfr. Hartmann–Jueptner–Matalonga et al. 2023.

130. Cfr. Bradford 2023; Finocchiaro 2024; Marchetti–Parona 2022; Roberts–Cowls–Hine et al. 2023.

131. Si vedano in particolare le categorie identificate dall'*Annex III* dell'*AI Act*.

categorie tradizionali[132]. In tal senso, il diritto pubblico comparato offre un importante contributo per l'analisi giuridica di un fenomeno complesso, che si inserisce nelle più ampie dinamiche del diritto costituzionale c.d. globale o transnazionale[133]. Come discusso, le problematiche sollevate dall'uso dei droni nelle emergenze non sono del tutto inedite, in quanto il diritto costituzionale ha avuto modo di affrontare le medesime criticità da altre prospettive, come per esempio il rispetto dei principi di trasparenza ed eguaglianza e dei diritti fondamentali nella disciplina giuridica dell'intelligenza artificiale, oppure i limiti al potere esecutivo nella disciplina costituzionale dello stato di emergenza. Inoltre, lo studio di tale fenomeno, così come la sua regolamentazione, rende inevitabile un'apertura ad altri saperi, dentro e fuori i confini del diritto, in una prospettiva interdisciplinare su cui il diritto comparato ha a lungo discusso, maturando importanti riflessioni circa le opportunità e i rischi dell'interdisciplinarietà[134]. A ciò si aggiunge il ruolo centrale che potrebbe assumere il metodo della comparazione secondo alcune delle sue classiche funzioni di acquisizione e verifica delle conoscenze[135] e di classificazione e individuazione di modelli che potrebbero diventare oggetto di circolazione[136].

In conclusione, dall'analisi qui svolta emerge chiaramente come la prospettiva del diritto pubblico comparato, sia sotto il profilo teorico che metodologico, costituisca una ricchezza irrinunciabile per un futuro sviluppo della regolamentazione dei droni nelle emergenze, così che questi costituiscano un beneficio per la società secondo i principi del costituzionalismo[137].

Riferimenti bibliografici

B. Ackerman (2004), *The Emergency Constitution*, in "The Yale Law Journal", vol. 113, 2004, n. 5

P. Adams, J. Lukiv (2025), *Ukraine Drones Strike Bombers during Major Attack in Russia*, in www.bbc.com, 6 February 2025

M. Ali, H. Duggal (2025), *Charting the Past Year of Russian Drone and Missile Attacks on Ukraine*, in www.aljazeera.com, 12 September 2025

J.A. Alic (1994), *The Dual Use of Technology: Concepts and Policies*, in "Technology in Society", vol. 16, 1994

D. Amoroso (2025), *La disciplina dei sistemi d'arma autonomi nel diritto internazionale umanitario. Stato dell'arte e prospettive di regolamentazione*, in "Rivista italiana di informatica e diritto", 2025, n. 2

D. Amoroso (2024), *Sistemi di supporto alle decisioni basati sull'IA e crimini di guerra: alcune riflessioni alla luce di una recente inchiesta giornalistica*, in "Diritti Umani e Diritto Internazionale", vol. 18, 2024

D. Amoroso, B. Giordano (2019), *Who Is to Blame for Autonomous Weapons Systems' Misdoings?*, in E. Carpanelli, N. Lazzerini (eds.), "Use and Misuse of New Technologies. Contemporary Challenges in International and European Law", Springer, 2019

D. Amoroso, G. Tamburini (2019), *I sistemi robotici ad autonomia crescente tra etica e diritto: quale ruolo per il controllo umano?*, in "BioLaw Journal – Rivista Di BioDiritto", 2019, n. 1

K. Anderson, M.C. Waxman (2019), *Legal-Policy Challenges of Armed Drones and Autonomous Weapon*

132. Si veda per esempio la riflessione maturata da Casonato 2020, p. 30.
133. Sul punto si rimanda in particolare Ferrari 2023.
134. Si pensi per esempio ai recenti contributi di Vedaschi 2021 e Resta 2024.
135. Cfr. de Vergottini 2022, p. 52 ss.; Bognetti 2015.
136. Così come suggerito anche in Casonato 2022, pp. 177-178.
137. Cfr. Cowls–Tsamados–Taddeo–Floridi 2021.

Systems, in J. Gow, E. Dijxhoorn, R.C. Kerr, G. Verdirame (eds.), "Routledge Handbook of War, Law and Technology", Routledge, 2019

P. Asaro (2020), *Autonomous Weapons and the Ethics of Artificial Intelligence*, in M. Liao (ed.), "Ethics of Artificial Intelligence", Oxford University Press, 2020

N. Bayomi, J.E. Fernandez (2023), *Eyes in the Sky: Drones Applications in the Built Environment under Climate Change Challenges*, in "Drones", vol. 7, 2023

C. Bassu (2010), *Terrorismo e costituzionalismo. Percorsi comparati*, Giappichelli, 2010

BBC News (2025), *Airport Drone Attacks Seem Professional, Says Danish Minister, But No Evidence of Russian Action*, in www.bbc.com, 25 September 2025

A. Beduschi (2022), *Harnessing the Potential of Artificial Intelligence for Humanitarian Action: Opportunities and Risks*, in "International Review of the Red Cross", vol. 104, 2022

P. Benvenuti (2007), *Judicial Review nella guerra al terrorismo nella decisione della Corte suprema israeliana sui targeted killings*, in "Diritto Pubblico Comparato ed Europeo", spec. XVIII, 2007

P.L. Bergen, D. Rothenberg (eds.) (2014), *Drone Wars. Transforming Conflict, Law, and Policy*, Cambridge University Press, 2014

A. Blanchard, C. Novelli, L. Floridi, M. Taddeo (2025), *A Risk-Based Regulatory Approach to Autonomous Weapon Systems*, in "Digital Society", vol. 4, 2025, n. 1

A. Blanchard, C. Novelli, L. Floridi, M. Taddeo (2024), *Autonomous Weapon Systems and Jus Ad Bellum*, in "AI & Society", vol. 39, 2024

G. Bognetti (2015), *Diritto costituzionale comparato. Un approccio metodologico*, Mucchi Editore, 2015

P. Bonetti (2006), *Terrorismo, emergenza e costituzioni democratiche*, il Mulino, 2006

L. Bonifati (2025), *I droni umanitari nei contesti di emergenza: un'analisi comparata a partire dal caso ucraino*, in "DPCE Online", vol. 70, 2025

M.J. Boyle (2015), *The Legal and Ethical Implications of Drone Warfare*, in "The International Journal of Human Rights", vol. 19, 2015

A. Bradford (2023), *Digital Empires: The Global Battle to Regulate Technology*, Oxford University Press, 2023

P.F. Bresciani, M. Palmirani (2024), *Constitutional Opportunities and Risks of AI in the Law-Making Process*, in "federalismi.it", 2024, n. 2

R. Brooks (2014), *Drones and the International Rule of Law*, in "Ethics & International Affairs", vol. 28, 2014

E. Calcagno, A. Marrone (eds.) (2023), *Above and Beyond: State of the Art of Uncrewed Combat Aerial Systems and Future Perspectives*, Istituto Affari Internazionali, 2023

I. Casey, A. Boyd (2025), *Romania Becomes Second NATO Country to Report Russian Drone in its Airspace*, in www.bbc.com, 14 September 2025

S. Casey-Maslen, M. Homayounnejad, H. Stauffer, N. Weizmann (2018), *Drones and Other Unmanned Weapons Systems under International Law*, Brill Nijhoff, 2018

A. Cassese (2007), *On Some Merits of the Israeli Judgement on Targeted Killings*, in "Journal of International Criminal Justice", 2007

A. Charlish, L. Kelly, B. Erling (2025), *Poland Downs Drones in its Airspace, Becoming First NATO Member to Fire During War in Ukraine*, in www.reuters.com, 10 September 2025

T. Chengeta (2021), *Autonomous Armed Drones and the Challenges to Multilateral Consensus on Value-Based Regulation*, in C. Enemark (ed.), "Ethics of Drone Strikes", Edinburgh University Press, 2021

C. Casonato (2022), *L'intelligenza artificiale e il diritto pubblico comparato ed europeo*, in "DPCE online", vol. 51, 2022, n. 1

C. Casonato (2020), *Per una intelligenza artificiale costituzionalmente orientata*, in Id. (ed.), "Pluralismo nel diritto costituzionale comparato", 2020

D. Cortright, R. Fairhurst, K. Wall (eds.) (2015), *Drones and the Future of Armed Conflict: Ethical, Legal, and Strategic Implications*, The University of Chicago Press, 2015

J. Cowls, A. Tsamados, M. Taddeo, L. Floridi (2021), *A Definition, Benchmark and Database of AI for Social Good Initiatives*, in "Nature Machine Intelligence", vol. 3, 2021, n. 2

R. Csernatoni (2018), *Constructing the EU's High-Tech Borders: FRONTEX and Dual-Use Drones for Border Management*, in "European Security", vol. 27, 2018, n. 2

C. Cucco, D. Mauri (2018), *Omicidi mirati a mezzo drone: brevi riflessioni a margine del caso "Lo Porto" tra diritto penale e diritto internazionale*, in "Diritto Penale Contemporaneo", 2018

B. Custers (ed.) (2016), *The Future of Drone Use. Opportunities and Threats from Ethical and Legal Perspectives*, Springer, 2016

G. De Gregorio (2022), *Digital Constitutionalism in Europe*, Cambridge University Press, 2022

F. de Londras (2022), *The Practice and Problems of Transnational Counter-Terrorism*, Cambridge University Press, 2022

G. de Vergottini (2022), *Diritto costituzionale comparato*, Wolters Kluwer, 2022

G. de Vergottini (2004), *Guerra e costituzione. Nuovi conflitti e sfide alla democrazia*, il Mulino, 2004

G. Delledonne (2023), *History and Concepts of Emergency*, in "Max Planck Encyclopedia of Comparative Constitutional Law", 2023

L.A. Dimatteo, C. Poncibò, M. Cannarsa (eds.) (2022), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics,* Cambridge University Press, 2022

E. Di Nucci, F. Santoni de Sio (eds.) (2016), *Drones and Responsibility: Legal, Philosophical, and Socio-technical Perspectives on Remotely Controlled Weapons*, Ashgate, 2016

F. Donati, G. Finocchiaro, F. Paolucci, O. Pollicino (a cura di) (2025), *La disciplina dell'intelligenza artificiale*, Giuffrè, 2025

D. Dyzenhaus (2012), *States of Emergency*, in M. Rosenfeld, A. Sajó (eds.), "The Oxford Handbook of Comparative Constitutional Law", Oxford University Press, 2012

C. Egger (2024), *The Politics and Spaces of Public-Private Partnerships in Humanitarian Tech Innovations*, in "EPC: Politics and Space", vol. 42, 2024

K.E. Eichensehr (2007), *On Target? The Israeli Supreme Court and the Expansion of Targeted Killings*, in "The Yale Law Journal", vol. 116, 2007

J.R. Emery (2016), *The Possibilities and Pitfalls of Humanitarian Drones*, in "Ethics & International Affairs", vol. 30, 2016

C. Enemark (2021), *Ethics of Drone Strikes: Restraining Remote-Control Killing*, Edinburgh University Press, 2021

J. Fardoulis, X. Depreytere, E. Sauvage, P. Gallien (2019), *Drones in the Desert: Augmenting HMA and Socio-Economic Activities in Chad*, in "Journal of Conventional Weapons Destruction", vol. 23, 2019

M. Fasan (2024), *Intelligenza artificiale e costituzionalismo contemporaneo: principi, diritti e modelli in prospettiva comparata*, Università degli Studi di Trento, 2024

G.F. Ferrari (2023), *I diritti nel costituzionalismo globale: luci e ombre*, Mucchi Editore, 2023

G. Fidone (2016), *Il partenariato pubblico privato: una fuga in avanti del legislatore nazionale rispetto al diritto europeo*, in "Diritto dell'Economia", vol. 29, 2016, n. 90

K. Finklea (2023), *Law Enforcement and Technology: Use of Unmanned Aircraft Systems*, Congressional Research Service, 2023

R.L. Finn, D. Wright (2016), *Privacy, Data Protection and Ethics for Civil Drone Practice: A Survey of Industry, Regulators and Civil Society Organisations*, in "Computer Law & Security Review", vol. 32, 2016, n. 4

G. Finocchiaro (2024), *The Regulation of Artificial Intelligence*, in "AI & Society", vol. 39, 2024, n. 4

M.S. Flaherty (2015), *The Constitution Follows the Drone: Targeted Killings, Legal Constraints, and Judicial Safeguards*, in "Public Policy", vol. 38, 2015

J. Forge (2010), *A Note on the Definition of 'Dual Use'*, in "Science and Engineering Ethics", vol. 16, 2010

M. Frau (2024), *I sistemi d'arma autonomi nel diritto pubblico*, Ledizioni, 2024

J. Galliott, D. MacIntosh, J.D. Ohlin (eds.) (2021), *Lethal Autonomous Weapons: Re-Examining the Law and Ethics of Robotic Warfare*, Oxford University Press, 2021

A. Gilli, M. Gilli (2016), *The Diffusion of Drone Warfare? Industrial, Organizational, and Infrastructural Constraints*, in "Security Studies", 2016, n. 1

A.R. Gonzales (2013), *Drones: The Power to Kill*, in "The George Washington Law Review", vol. 82, 2013, n. 1

E. Gosselin-Malo (2023), *Leonardo Displays Falco Xplorer Drone Armed with MBDA Missile*, in www.defensenews.com, 21 June 2023

J. Hartmann, E. Jueptner, S. Matalonga et al. (2023), *Artificial Intelligence, Autonomous Drones and Legal Uncertainties*, in "European Journal of Risk Regulation", vol. 14, 2023, n. 1

B. Heinrichs (2022), *Discrimination in the Age of Artificial Intelligence*, in "AI & Society", vol. 37, 2022, n. 1

K.J. Heller (2013), *'One Hell of a Killing Machine': Signature Strikes and International Law*, in "Journal of International Criminal Justice", vol. 11, 2013, n. 1

Human Rights Council (2025), *"They are Hunting Us": Systematic Drone Attacks Targeting Civilians in Kherson*, 28 May 2025

International Committee of the Red Cross (2020), *Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach*, in "International Review of the Red Cross", vol. 102, 2020

International Committee of the Red Cross (2006), *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare*, in "International Review of the Red Cross", vol. 88, 2006

J. Jaffer (2016), *The Drone Memos. Targeted Killings, Secrecy, and the Law*, New York Press, 2016

J. Karlsrud, F. Rosén (2018), *Lifting the Fog of War? Opportunities and Challenges of Drones in UN Peace Operation*', in K.B. Sandvik, M. Gabrielsen Jumbert (eds.), "The Good Drone", Routledge, 2018

M. Katrak, I. Chakrabarty (2023), *Privacy, Political Participation, and Dissent Facial Recognition Technologies and the Risk of Digital Authoritarianism in the Global South*, in A. Quintavalla, J. Temperman (eds.), "Artificial Intelligence and Human Rights", Oxford University Press, 2023

L. Kayali (2025), *NATO Isn't Ready for Russia's Drones*, in www.politico.eu, 12 September 2025

R.F. Khalil (2023), *Aerial Trespass and the Fourth Amendment*, in "Michigan Law Review", vol. 121, 2023, n. 7

R. Koslowski, M. Schulzke (2018), *Drones Along Borders: Border Security UAVs in the United States and the European Union*, in "International Studies Perspectives", vol. 19, 2018, n. 4

S. Kreps, P. Lushenko (2023), *Drones in Modern War: Evolutionary, Revolutionary, or Both?*, in "Defense & Security Analysis", vol. 39, 2023

S. Kreps, S. Maxey (2021), *Context Matters: The Transformative Nature of Drones on the Battlefield*, in G. Giacomello, F.N. Moro, M. Valigi (eds.), "Technology and International Relations", Edward Elgar Publishing, 2021

C. Kuner, M. Marelli (2020), *Handbook on Data Protection in Humanitarian Action*, International Committee of the Red Cross, 2020

D. Kunertova (2023), *Drones Have Boots: Learning from Russia's War in Ukraine*, in "Contemporary Security Policy", vol. 44, 2023

R. Kweera (2023), *Drones in Modern Warfare: Utilization in India-Pakistan Cross-Border Terrorism and Security Implications*, in "Strategic Analysis", vol. 47, 2023, n. 4

R. Liivoja, K.-R. Leins, T. McCormack (2016), *Emerging Technologies of Warfare*, in R. Liivoja, T. McCormack (eds.), "Routledge Handbook of the Law of Armed Conflict", Routledge, 2016

E. Longo, A. Pin (2023), *Oltre il costituzionalismo? Nuovi principi e regole costituzionali per l'era digitale*, in "Diritto Pubblico Comparato ed Europeo", vol. 25, 2023

M.G. Losano (2018), *Guerre ibride, omicidi mirati, droni: conflitti senza frontiere e senza diritto*, in L. Forni, T. Vettor (a cura di), "Sicurezza e libertà in tempo di terrorismo globale", Giappichelli, 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", vol. 51, 2022, n. 1

L. Marin (2017), *The Deployment of Drone Technology in Border Surveillance*, in M. Friedewald, J. Cas, R. Bellanova et al. (eds.), "Surveillance, Privacy and Security", Routledge, 2017

J.L. Mashaw (1976), *The Supreme Court's Due Process Calculus for Administrative Adjudication in Mathews v. Eldridge: Three Factors in Search of a Theory of Value*, in "The University of Chicago Law Review", vol. 44, 1976, n. 1

S. Massa (2025), *Peeping Town: Drone Surveillance and the Exclusionary Rule in Long Lake Township v. Maxon*, in "Northwestern University Law Review", vol. 119, 2025, n. 4

T. McFarland (2020), *Autonomous Weapon Systems and the Law of Armed Conflict*, Cambridge University Press, 2020

T. McFarland, T. McCormack (2014), *Mind the Gap: Can Developers of Autonomous Weapons Systems Be Liable for War Crimes?*, in "International Law Studies", vol. 90, 2014

C. Meloni, W. Patten, F. Borello et al. (2019), *Droni armati in Italia e in Europa: problemi e prospettive*, in "Diritto Penale Contemporaneo", 2019

N. Menéndez González (2023), *The Rights to Privacy and Data Protection and Facial Recognition Technology in the Global North*, in A. Quintavalla, J. Temperman (eds.), "Artificial Intelligence and Human Rights", Oxford University Press, 2023

N. Menéndez González, G. Mobilio (2025), *Between Prohibited Risks and High Risks: The Regulation of Facial Recognition Technology*, in O. Pollicino, F. Donati, G. Finocchiaro, F. Paolucci. (a cura di), "La disciplina dell'intelligenza artificiale", Giuffrè, 2025

L. Merla (2016), *Droni, privacy e tutela dei dati personali*, in "Informatica e diritto", 2016, n. 1

G. Mobilio (2021), *Tecnologie di riconoscimento facciale: rischi per i diritti fondamentali e sfide regolative*, Editoriale Scientifica, 2021

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

S. Miller (2018), *Dual Use Science and Technology, Ethics and Weapons of Mass Destruction*, Springer, 2018

S.A.H. Mohsan, Q.A. Zahra, M.A. Khan et al. (2022), *Role of Drone Technology Helping in Alleviating the COVID-19 Pandemic*, in "Micromachines", vol. 13, 2022

C. Nardocci (2024), *La (seconda) svolta del 2024. Anche il Consiglio d'Europa decide di regolamentare l'intelligenza artificiale*, in "BioLaw Journal – Rivista di BioDiritto", 2024, n. 1 sp.

H. Nasu, R. McLaughlin (2014), *Challenges of New Technologies for the Law of Armed Conflict*, in H. Nasu, R. McLaughlin (eds.), "New Technologies and the Law of Armed Conflict", T.M.C. Asser Press, 2014

F.N. Okpaleke, B. Nwosu, C.R. Okoli, E.E. Olumba (2023), *The Case for Drones in Counter-Insurgency Operations in West African Sahel*, in "African Security Review", vol. 32, 2023

F. Paolucci (2025), *Constitutional Safeguards in the Age of AI. A Study on the Fundamental Rights Impact Assessment of Facial Recognition Technology*, Bocconi University, 2025

D.N. Pearlstein (2013), *Enhancing Due Process in Targeted Killing*, in "American Constitution Society for Law and Policy", 2013

J. Penney, S. McKune, L. Gill, R. Deibert (2018), *Advancing Human-Rights-By-Design in the Dual-Use Technology Industry*, in "Journal of International Affairs", vol. 71, 2018

V. Piergigli (2023), *Diritto costituzionale dell'emergenza*, Giappichelli, 2023

V. Piergigli (2023-a), *Potere e stato di emergenza*, in "Enciclopedia del Diritto", 2023

M. Pizzi, M. Romanoff, T. Engelhardt (2020), *AI for Humanitarian Action: Human Rights and Ethics*, in "International Review of the Red Cross", vol. 102, 2020

A. Pizzorusso (1993), *Emergenza, stato di*, in "Enciclopedia delle Scienze Sociali", 1993

S.V. Pustovit, E.D. Williams (2010), *Philosophical Aspects of Dual Use Technologies*, in "Science and Engineering Ethics", vol. 16, 2010

A. Quintavalla (2025), *Protezione dei diritti umani e intelligenza artificiale: un'analisi critica del regolamento europeo sui prodotti a duplice uso*, in "Rivista italiana di informatica e diritto", 2025, n. 2

A. Quintavalla, J. Temperman (eds.) (2023), *Artificial Intelligence and Human Rights*, Oxford University Press, 2023

A. Rejeb, K. Rejeb, S. Simske, H. Treiblmaier (2021), *Humanitarian Drones: A Review and Research Agenda*, in "Internet of Things", vol. 16, 2021

G. Resta (2024), *"So Lonely": Comparative Law and the Quest for Interdisciplinary Legal Education*, in "International Journal for the Semiotics of Law - Revue internationale de Sémiotique juridique", vol. 37, 2024, n. 5

A.-M. Reynaers, S. Grimmelikhuijsen (2015), *Transparency in Public–Private Partnerships: Not So Bad After All?*, in "Public Administration", vol. 93, 2015, n. 3

H. Roberts, J. Cowls, E. Hine et al. (2023), *Governing Artificial Intelligence in China and the European Union: Comparing Aims and Promoting Ethical Outcomes*, in "The Information Society", vol. 39, 2023

G. Rohi, O. Ejofodomi, G. Ofualagba (2020), *Autonomous Monitoring, Analysis, and Countering of Air Pollution Using Environmental Drones*, in "Heliyon", vol. 6, 2020

N. Ronzitti (2019), *Diritto internazionale dei conflitti armati*, Giappichelli, 2019

M. Rostami, A. Farajollahi, H. Parvin (2024), *Deep Learning-Based Face Detection and Recognition on Drones*, in "Journal of Ambient Intelligence and Humanized Computing", vol. 15, 2024, n. 1

I.S. Rubinstein (2011), *Regulating Privacy by Design*, in "Berkeley Technology Law Journal", vol. 26, 2011, n. 3

M. Sassoli (2024), *International Humanitarian Law*, Edward Elgar Publishing, 2024

D. Saxon (ed.) (2013), *International Humanitarian Law and the Changing Technology of War*, Brill, 2013

M. Schulzke (2019), *Drone Proliferation and the Challenge of Regulating Dual-Use Technologies*, in "International Studies Review", vol. 21, 2019, n. 3

V. Sehrawat (2021), *Drones and the Law*, Emerald Publishing, 2021

G.D. Solis (2016), *The Law of Armed Conflict. International Humanitarian Law in War*, Cambridge University Press, 2016

E. Stradella (2022), *Le fonti nel diritto comparato: analisi di scenari extraeuropei (Stati Uniti e Cina)*, in "DPCE Online", vol. 51, 2022, n. 1

N. Suzor, M. Dragiewicz, B. Harris et al. (2019), *Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online*, in "Policy & Internet", vol. 11, 2019

M. Taddeo (2024), *The Ethics of Artificial Intelligence in Defence*, Oxford University Press, 2024

T.T. Takahashi (2013), *Drones and Privacy*, in "Science and Technology Law Review", vol. 14, 2013, n. 1

A.A. Tarr, A.G. Perera, J. Chahl et al. (2022), *Drones—Healthcare, Humanitarian Effort and Recreational Use*, in A.A. Tarr et al. (eds.), "Drone Law and Policy: Global Development, Risks, Regulation and Insurance", Routledge, 2022

UNOCHA (2014), *Unmanned Aerial Vehicles in Humanitarian Response*, in "OCHA Policy and Studies Series", vol. 10, 2014

A. Van Wynsberghe, T. Comes (2020), *Drones in Humanitarian Contexts, Robot Ethics, and the Human–Robot Interaction*, in "Ethics and Information Technology", vol. 22, 2020

A. Vedaschi (ed.) (2024), *Governmental Policies to Fight Pandemic*, Brill, 2024

A. Vedaschi (2022), *Guerra e Costituzioni: spunti dalla comparazione*, in "Osservatorio Costituzionale", 2022, n. 3

A. Vedaschi (2021), *Diritto comparato e interdisciplinarietà: tra innata vocazione e incompiuta realizzazione?*, in "Diritto Pubblico Comparato ed Europeo", 2021, n. 2

A. Vedaschi (2011), *Osama bin Laden: l'ultimo targeted killing. Gli Stati Uniti hanno dunque la licenza di uccidere?*, in "Diritto Pubblico Comparato ed Europeo", 2011, n. 3

A. Vedaschi (2007), À la guerre comme à la guerre? *La disciplina della guerra del diritto costituzionale comparato*, Giappichelli, 2007

A. Vedaschi, C. Graziani (2025), *Artificial Intelligence, Counter-Terrorism and the Rule of Law*, Edward Elgar, 2025

S.I. Vladeck (2014), *Targeted Killing and Judicial Review*, in "The George Washington Law Review Arguendo", vol. 82, 2014

M. Christen, M. Hunt, N. Biller-Andorno, (2022) *Supporting Value Sensitivity in the Humanitarian Use of Drones through an Ethics Assessment Framework*, in "International Review of the Red Cross", vol. 104, 2022

S. Wachter (2018), *The GDPR and the Internet of Things: A Three-Step Transparency Model*, in "Law, Innovation and Technology", vol. 10, 2018, n. 2

R. Weaver (2021), *The Constitutional Implications of Drones, Facial Recognition Technology and CCTV*, in "Public Governance, Administration and Finances Law Review", 2021, n. 2

S. Weill (2016), *Reducing the Security Gap through National Courts: Targeted Killings as a Case Study*, in "Journal of Conflict and Security Law", vol. 21, 2016

S. Weill (2014), *The Role of National Courts in Applying International Humanitarian Law*, Oxford University Press, 2014

D. Whetham (2015), *Drones to Protect*, in "The International Journal of Human Rights", vol. 19, 2015

S. Wilder (2022), *In Ukraine, Humanitarian Drones Can Save Lives*, in www.aljazeera.com, 2022

L.E. Willis (2014), *Why Not Privacy by Default?*, in "Berkeley Technology Law Journal", vol. 29, 2014, n. 1

F.J. Zuiderveen Borgesius (2020), *Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence*, in "The International Journal of Human Rights", vol. 24, 2020, n. 10

Sezione monografica

Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement

a cura di

Gaetana Morgante e Gaia Fiorinelli

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0244 • articolo non sottoposto a peer review • pubblicato in anteprima il 27 gen. 2026

Gaetana Morgante – Gaia Fiorinelli

Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e *law enforcement*

Introduzione

G. Morgante è professoressa ordinaria in Diritto penale alla Scuola Superiore Sant'Anna di Pisa
G. Fiorinelli è ricercatrice t.d. in Diritto penale alla Scuola Superiore Sant'Anna di Pisa

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement - Parte 1*, a cura di Gaetana Morgante e Gaia Fiorinelli

La sezione monografica "Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement" raccoglie i contributi di diversi *team* di ricerca coinvolti nel Progetto PNRR "Partenariato Esteso" PE7 *SERICS – SEcurity and RIghts in the CyberSpace*, finanziato dall'Unione europea – Next Generation EU – Spoke 1 – *CybeRights* – WP4 (*Cybercrime e Cyberdiplomacy*).

In particolare, il gruppo di ricerca multidisciplinare afferente al WP4 – che riunisce la Scuola Superiore Sant'Anna di Pisa, l'Università di Trento, l'Università degli Studi di Napoli Federico II, l'Università degli Studi di Verona e l'Università degli Studi di Milano – contribuisce allo sviluppo di un concetto integrato e olistico di cybersicurezza, quale obiettivo generale del progetto *CybeRights*, mediante le competenze e gli strumenti concettuali del diritto penale sostanziale e processuale, della criminologia, del diritto internazionale e delle scienze politiche e strategiche.

La transizione digitale che connota in modo pervasivo l'epoca attuale esercita, infatti, un profondo impatto sul fenomeno criminale, generando nuove vulnerabilità, nuove opportunità delittuose e dinamiche inedite di vittimizzazione, che si manifestano in uno spazio strutturalmente svincolato dai confini geografici e giurisdizionali. In questa prospettiva, i modelli penalistici di prevenzione e contrasto dei reati informatici, ai danni di individui, imprese, amministrazioni pubbliche e infrastrutture critiche, richiedono un ripensamento sostanziale, in dialogo costante con la ricerca criminologica, al fine di elaborare strumenti di tutela più efficaci e concettualmente solidi. Parallelamente, il panorama delle fonti sollecita un rinnovato sforzo di sistemazione teorica, sviluppandosi entro strutture multilivello sempre più articolate, che sovrappongono cooperazione internazionale, armonizzazione europea e interventi nazionali, ai quali si affiancano forme di regolazione privatistica o tecnologica, in un quadro di co-regolazione pubblico-privata. A fronte di un "arsenale" penalistico così articolato, l'analisi dei dati giudiziari restituisce, per converso, con particolare efficacia le difficoltà di *enforcement* del diritto penale nel cyberspazio, a partire dalle criticità nell'identificazione degli autori dei reati, nell'attribuzione degli attacchi e, in definitiva, nell'emersione di un fenomeno criminale che rimane caratterizzato da una consistente cifra oscura.

Del resto, la transizione digitale produce altresì un significativo impatto sui profili procedurali e sui poteri e mezzi d'indagine, aprendo a nuove modalità d'investigazione sui reati informatici (e non): accanto a un'inedita esigenza di standardizzazione delle tecniche di raccolta, conservazione e utilizzazione delle prove digitali, ciò pone l'urgente necessità di un bilanciamento di tali pratiche con la salvaguardia dei diritti fondamentali. Invero, la digitalizzazione dei poteri investigativi contribuisce indubbiamente al (necessario) incremento della loro efficienza ed efficacia, ma impone di mitigarne la strutturale intrusività, nel complesso scenario della cooperazione internazionale, europea e pubblico-privata.

Proprio con riferimento a quest'ultimo profilo, non può trascurarsi come la criminalità digitale assuma progressivamente un rilievo sempre maggiore al livello delle relazioni internazionali e delle dinamiche geopolitiche, collocandosi in un'area di confine in cui sfumano le distinzioni tra atti criminali e atti di natura bellica, mentre anche la morfologia delle sanzioni si trasforma (si pensi, ad esempio, al c.d. *EU Cyber Diplomacy Toolbox*, che ha istituito forme di risposta sul piano *diplomatico* rispetto alle attività informatiche dolose). Il diritto internazionale si intreccia così stabilmente con il diritto penale sostanziale e processuale, quale piano della cooperazione ma anche quale autonoma fonte di disciplina delle condotte nel cyberspazio, richiedendo lo sviluppo di strumenti analitici per interpretare le tendenze emergenti e i futuri scenari di applicazione delle tecnologie informatiche alla sicurezza e alla difesa internazionale.

Nelle prospettive indicate, lo stesso concetto di cybersicurezza si scompone in un prisma di significati: (nuovo) bene giuridico da tutelare, condizione per la protezione dei diritti individuali e collettivi nel cyberspazio, fondamento e limite delle indagini digitali, nonché dimensione strategica per il diritto e le relazioni internazionali.

I contributi raccolti in questa Sezione monografica si inseriscono in questo quadro, con l'obiettivo di offrire una prospettiva critica sulle trasformazioni del fenomeno criminale nello spazio digitale, sulla necessità di un assestamento concettuale e assiologico nel diritto penale, sulle nuove dimensioni della cooperazione e sull'applicazione del diritto internazionale, nonché sul ruolo delle piattaforme digitali e sul coordinamento dei poteri investigativi nel rispetto delle garanzie costituzionali dell'ordinamento multilivello.

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0254 • articolo sottoposto a peer review • pubblicato in anteprima il 15 dic. 2025

Gaetana Morgante

Transizione digitale e diritto penale. Dall'evoluzione delle categorie sostanziali al "nuovo volto" del law enforcement

L'impatto della transizione digitale sul diritto penale può essere apprezzato sul duplice versante del diritto sostanziale e del law enforcement. Pur a fronte di una tendenziale anelasticità del diritto penale agli effetti trasformativi di passaggi *disruptive,* l'evoluzione delle categorie sostanziali – dal soggetto attivo, alla condotta, dalla causalità alla colpevolezza – risulta inevitabile. La pervasività degli effetti della transizione digitale, infatti, si riverbera sui modelli di incriminazione e sui presupposti di imputazione di una responsabilità storicamente e strutturalmente legata alla prospettiva della persona fisica, dello spazio "analogico" e della fondazione antropomorfica delle categorie sostanziali. Come paradigmaticamente desumibile dai profili penali della cybersecurity, la trasformazione delle categorie sostanziali e dei presupposti della responsabilità si collega anche alla sperimentazione di nuovi percorsi di law enforcement, caratterizzati dall'enfasi sulle funzioni preventive e collaborative tra i diversi attori del mondo digitale.

Transizione digitale – Responsabilità penale – Cybercrime – Cybersecurity – Law enforcement

Digital transition and criminal law. From the evolution of substantive categories to the "new face" of the law enforcement

The impact of the digital transition on criminal law can be appreciated under two different perspectives: substantive law and law enforcement. Despite the tendency of criminal law to be inelastic to the transformative effects of changes that are disruptive, the evolution of substantive categories – from the author of the crime to the conduct, from causality to culpability – is unavoidable. The pervasiveness of the effects of the digital transition impacts on models of criminalization and on the prerequisites for attributing responsibility historically and structurally linked to the perspective of the natural person, the "analog" space, and the anthropomorphic foundation of substantive categories. As can be paradigmatically inferred from the analysis of the criminal issues of cybersecurity, the transformation of the substantive categories and elements of liability is also linked to new approaches to law enforcement, characterized by an emphasis on preventive and collaborative functions between the various actors of the digital world.

Digital transition – Criminal responsibility – Cybercrime – Cybersecurity – Law enforcement

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

La ricerca si inserisce nell'ambito del Progetto PNRR "Partenariato Esteso" PE 7 SERICS Security and Rights in the Cyber Space/ Spoke 1: Progetto CybeRights Codice identificativo: M4C2 11.3 - PE0000014 - CUPJ53C22003110001

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement - Parte 1*, a cura di Gaetana Morgante e Gaia Fiorinelli

1. Transizione digitale ed effetti trasformativi sulle categorie penalistiche

La transizione digitale esprime in termini, per così dire, immaginifici il carattere pervasivo e totale dell'impatto della tecnologia in ambito sociale, economico, produttivo, pubblico e privato. Il riferimento alla "transizione" appare, ai fini che qui interessano, singolarmente pertinente all'analisi delle conseguenze sulle categorie giuridiche e, in particolare, penalistiche della digitalizzazione in quanto rimanda a quel "passaggio" da un mondo analogico ad un mondo *digital-based* che si riflette anche nell'evoluzione delle chiavi interpretative dei presupposti sostanziali della responsabilità penale e dei relativi percorsi di law enforcement. La categoria concettuale della "transizione" rimanda, infatti, ad un dualismo che può essere declinato sia nei termini diacronici del "prima" e del "dopo" sia in quelli sincronici del gemellaggio in linea con quel paradigma del *digital twin* secondo il quale la digitalizzazione avrebbe creato "gemelli" di mondi ma soprattutto di diritti a vario titolo speculari rispetto a quelli del mondo analogico[1], come nei casi paradigmatici dei binomi sicurezza pubblica e cybersecurity oppure identità personale e digitale[2]. La prospettiva che viene prevalentemente in considerazione è quella di una sorta di diritto del metaverso[3] ove principi, regole, fattispecie e, ai fini che qui più interessano, modelli di incriminazione

1. Sul predetto "sdoppiamento" dei diritti v. T.E. Frosini 2020, p. 1. e V. Frosini 2000, p. 275, Iannuzzi 2024, p. 36 ss.
2. V. Iannuzzi–Laviola 2023, p. 9 ss.
3. Per un'analisi delle connessioni tra metaverso e trasformazioni del diritto v. Riccio 2023, p. 2 ss. ove si fa, per l'appunto, riferimento alla *Second Life* che, nella prospettiva estensiva sopra delineata, amplia le possibilità fisiche, per mezzo dell'affidamento allo strumento tecnologico. In argomento v. anche Sarzana di Sant'Ippolito–Pierro–Epicoco 2022, p. 50, Sciancalepore 2023, Incampo 2025, p. 59 ove si esaminano le conseguenze della necessaria spazializzazione del diritto e della dogmatica giuridica sulla a-spazializzazione indotta dalla transizione digitale. Sulle trasformazioni delle soggettività giuridiche v. Cheong 2022, p. 467 ss., Haber 2024, p. 843-891. Sulle intersezioni con i profili penali della cybersecuity con particolare riguardo all'individuazione dei responsabili dei reati, Razzante 2022, p. 216.

siano duplicati in una seconda e inedita vita dai contorni ampiamente derogatori e potenzialmente "sregolati" rispetto a quella "reale".

Se però la metafora del gemellaggio può risultare concettualmente e, soprattutto, assiologicamente compatibile con una prospettiva di estensione dei diritti di fronte alla crescente complessità indotta dalle trasformazioni, *rectius* transizioni, tecnologiche, la traslazione della nozione di *digital transition* all'universo penalistico risulta molto più ardua in ragione dell'incompatibilità di principio tra la portata "totalizzante"[4] della trasformazione tecnologica e la necessaria frammentarietà delle scelte di politica criminale. A fronte del carattere capillare degli effetti del *fenomeno* tecnologico, il diritto penale è innanzi tutto chiamato a punire singoli e concreti *fatti* (pur) commessi in ambiente digitale. Tale frammentarietà si declina altresì in una tendenziale, o quantomeno iniziale, anelasticità del diritto penale di fronte ai cambiamenti totali come ravvisabile nei settori diversi, se pur concettualmente limitrofi, dell'ambiente o del lavoro fortemente influenzati dal progresso scientifico e produttivo, i quali sono trasversalmente percorsi da quel progresso tecnologico che sfida la tenuta delle categorie generali del diritto penale sostanziale.

La menzionata tendenziale anelasticità del diritto penale di fronte alle trasformazioni totali può essere apprezzata tanto su un piano extrasistematico, ovvero di profili che investono elementi di contesto di rilievo non strettamente penalistico, quanto a livello intrasistematico con particolare riguardo a quelle categorie penalistiche sostanziali (soggetto attivo, condotta, colpevolezza) o processuali dalla natura storicamente umanizzata e antropomorfica e, come tali, resistenti alle forme di smaterializzazione indotte dalla transizione digitale.

Sul piano extrasistematico l'elemento che esprime in termini più significativi l'impatto della *digital transition* sul diritto (anche) penale è quello del *rischio* o, più correttamente, della generazione di nuovi profili di rischio connessi alla digitalizzazione di attività individuali, produttive e pubbliche[5]. Pur non trattandosi di un profilo extrasistematico di nuova emersione a seguito della transizione digitale, essendo, come ricordato, coessenziale ad altre forme di trasformazione, o rivoluzione, scientifica o produttivo-industriale, la proliferazione dei rischi connessi all'avvento della digitalizzazione ha assunto, ai fini dell'analisi del relativo impatto sul diritto penale, caratteri di ancora maggiore pervasività dal momento che la crescente complessità di processi e attività mediate dalla tecnologia e il *gap* di conoscenza dei presupposti di funzionamento ed operatività della stessa (o *digital divide*) ha dato luogo a forme di vulnerabilità del tutto inedite le quali, prevalentemente tematizzate sul versante – *lato sensu* fisiologico e positivo – dei diritti[6], risultano in una parallela dimensione – patologica e negativa – di prevenzione e contrasto delle nuove forme di offesa agli stessi, coessenziali a disvelare la necessità di nuovi spazi e modi di intervento del diritto penale.

Dal punto di vista della riflessione teorica, come ricordato, si tratta di uno scenario non del tutto sconosciuto in quanto più in generale riferibile all'analisi degli effetti delle trasformazioni indotte dal progresso scientifico-tecnologico, per l'appunto, sulla generazione di nuove forme di offesa agli interessi meritevoli di tutela penale e sulla necessità di concettualizzare nuove forme di "coesistenza" tra pericolo e utilità sociale di attività tecnologicamente avanzate[7]. Come ampiamente esaminato nel settore, che con quello ambientale condivide alcuni tratti comuni con il tema oggetto della

4. In questi termini v. Garapon–Lassegue 2021, p. 79. Per un'ulteriore analisi della trasformazione della funzione giurisdizionale a fronte della trasformazione tecnica v. Longo 2023, p. 47 ss. ove si esamina il tema dello sviluppo del processo digitalizzato "per comprenderne la sostenibilità, anzitutto in termini costituzionali".
5. Per una compiuta concettualizzazione dell'effetto *disruptive* e totalizzante del progresso tecnologico sulla generazione di nuovi profili di rischio v. Beck 2000.
6. In questa prospettiva di valutazione dei "rischi" di nuove ed inedite offese e limitazioni dei diritti umani v. Sartor 2017, p. 424 ss., che riconduce all'impiego delle tecnologie informatiche anche effetti (sociali e di potenziale rilevanza penale) negativi, tra i quali: disoccupazione, alienazione, disuguaglianze, sorveglianza (da parte di soggetti pubblici e privati), profilazione, condizionamenti, discriminazione, esclusione sociale, forme inedite di censura.
7. Per una riflessione sui nuovi profili di rischio penalmente rilevante nel settore del diritto ambientale v. Gargani 2019, p. 111 ss., ove si dà conto di come "la determinazione dell'oggetto e dei limiti di tutela" assuma

presente indagine, del diritto penale del lavoro la progressiva emersione della nozione di "rischio", non solo come ulteriore anticipazione della soglia dell'intervento ma come elemento coessenziale e, soprattutto, non eliminabile dalle potenziali fonti di offesa dei beni giuridici rilevanti, ha condotto ad una rapida trasformazione dei confini delle categorie del diritto penale generale[8] passando dalla tralatizia logica binaria e, per così dire, ultimativa del dovere di eliminazione del pericolo come condizione per la prosecuzione dell'attività a quella plurale dell'obbligo collettivo di gestione di un rischio impossibile da azzerare.

Sul versante della variazione degli elementi intrasistematici, la transizione digitale e la pervasività delle trasformazioni tecnologiche induce significativi variazioni nella definizione del *soggetto attivo*, in considerazione della sua frequente invisibilità, *rectius* anonimato, dovuta alla mancanza di un *locus commissi delicti* fisico[9] e all'attitudine dell'ambientamento digitale del reato a fare da schermo alla sua identità, della delimitazione delle *condotte* in forza della necessaria variazione dei modelli di incriminazione[10] e, in diretta connessione con il tema del tendenziale anonimato del soggetto attivo, dei confini e degli stessi margini di operatività dell'accertamento dell'*elemento soggettivo*, peraltro prevalentemente di tipo doloso e quindi storicamente connesso a profili psicologici di ardua traslazione alla sfera digitale.

Posto che, dunque, alla riflessione penalistica non sia estranea l'esperienza di modificazioni, o rivoluzioni, con effetti *disruptive* sulle categorie giuridiche di riferimento della parte generale e speciale[11], il dato che differenzia potentemente la transizione digitale da altre forme, in parte note, di "rivoluzioni" scientifico-produttive è il carattere di totale immaterialità della transizione digitale, come tale astrattamente incompatibile con un diritto, quale quello penale, fortemente legato alla materialità e all'"ambientamento fisico-analogico" del soggetto attivo, della condotta, della colpevolezza e di ogni altro segmento della filiera della politica criminale e del law enforcement. Non stupisce, dunque, che la primigenia reazione a questo cambiamento sia stata quella dell'angoscia[12], della sottomissione[13] o dello smantellamento[14] dell'esistente rispetto a trasformazioni che paiono mettere in crisi la stessa praticabilità del diritto penale nell'affrontare i rischi e le nuove vulnerabilità emergenti in ambiente digitale.

Pur a fronte delle indubbie variazioni trasformative imposte dalla transizione digitale, il diritto penale si trova, tuttavia, di fronte ad una straordinaria opportunità di essere rifondato a partire dalle sue categorie concettuali di riferimento proprio nel nome dei principi fondamentali che ne informano l'esistenza valorizzando il contenuto di garanzia dinamica, e non statica, dei diritti fondamentali rispetto a nuove forme di aggressione. La caratterizzazione antropomorfica dei modelli di incriminazione, infatti, parrebbe poter essere, per così dire, riferita più alle tecniche di costruzione delle fattispecie che ai principi e alle funzioni del

"un'intrinseca processualità e relatività", non potendo la eventuale rilevanza penale della condotta essere apprezzata a priori, in base a parametri naturalistici e senza essere mediata dall'operatività di elementi giuridici extrapenali volti a stabilire "soglie" e presupposti di legittimità delle attività rischiose. In questi termini, si argomenta la natura "convenzionale" e non più "assoluta" della tutela. Sul punto cfr. anche De Francesco 2004, p. 62 ss.

8. Fondamentali le riflessioni sul tema di Padovani 1996, p. 1161.
9. In argomento si rinvia alla riflessione di Incampo 2025, p. 59 ove si ripercorrono le radici filosofiche giuridiche del collegamento tra diritto e spazio "E il diritto? Cosa accade al diritto? Il nomos è sempre stato, per dirla con Carl Schmitt, 'nomos della terra' [*Nomos der Erde*]. Lo stesso concetto kelseniano di 'validità' [*Geltung*] indica l'"esistenza specifica' [*speziphische Existenz*] di un fatto o di una norma in un tempo e in uno spazio determinati".
10. V. *infra* sub 2.
11. Sulle origini perfino mitologiche della connessione tra crime e technology v. McGuire 2012, p. 7 ss.; Smith 2004, p. 105 ss.
12. Stortoni 2004, p. 75, rispetto alla "asserita non conoscenza né conoscibilità del pericolo", con le relative ricadute di tale impostazione sugli stessi istituti della condotta, della causalità e della colpevolezza.
13. Bodei 2019.
14. Hoffmann–Riem 2020, p. 143 ss.

diritto penale che si rivelano molto più elastici dei modelli consolidati in quanto chiamati ad adattarsi al mondo, anche e soprattutto quello criminale, che cambia in una logica di strumentalità rispetto alla protezione dei beni giuridici e dei rispettivi titolari che non può venir meno sol che cambi il contesto nell'ambito del quale nuove offese sono perpetrate. Si tratta, invero, anche rispetto alla distinzione tra piano dei principi e piano degli strumenti di incriminazione, di una riflessione nota anche se ancora una volta riferita ad una, solo apparentemente, più limitata analisi delle modalità[15] della condotta o, per l'appunto, dello *strumento*[16] dell'azione, la quale, ben lontana dal poter essere confinata entro la nicchia dei diversi modi in cui un interesse meritevole di tutela può essere offeso, pone, nella materia che ci occupa, la necessità che il diritto penale si adatti alle trasformazioni dei modelli di incriminazione acquisendo anche nel *cyberspace* una condizione di esistenza pur con forme completamente rinnovate[17].

2. I modelli di incriminazione dei reati commessi in ambiente digitale

La richiamata caratterizzazione anelastica del diritto penale sul piano dei diversi modelli di incriminazione è ravvisabile nella prima concettualizzazione[18] del c.d. *computer crime*. Nel quadro di una definizione saldamente "ancorata" ad un supporto "fisico", il *pattern* di riferimento era stato individuato nell'*abuso* ravvisato, nel più ampio scenario del valore dell'informazione generata e circolata grazie alle tecnologie informatiche, in "any illegal, unethical or unauthorized behaviour relating to the automatic processing and transmission of data". Invero, non stupisce che il modello di riferimento si sia attestato su una figura, quella dell'abuso, per un verso "fondazionale" della teoria generale del diritto e, per altro verso, facente leva su una sorta di modello "minimale" di diritto penale sanzionatorio *ex post* della violazione delle regole d'uso (definite *aliunde*) di sistemi che così prepotentemente si affermavano in conseguenza della rivoluzione delle tecnologie informatiche. In questa prima tranquillizzante definizione del reato commesso in ambiente digitale l'indicazione politico-criminale si attesta su solchi arati da millenni quali quelli dei *reati contro il patrimonio* nella duplice caratterizzazione delle *condotte di sottrazione* (l'immissione, l'alterazione, la cancellazione e/o la soppressione di dati informatici e/o programmi informatici eseguita volontariamente, con l'intento di commettere un trasferimento illegale di fondi o qualsiasi altro bene e la violazione del diritto esclusivo del titolare di un programma informatico protetto, con l'intento di sfruttare commercialmente il programma e immetterlo sul mercato) e *di intrusione/danneggiamento* (l'immissione, l'alterazione, la cancellazione e/o la soppressione di dati informatici e/o programmi informatici compiuta intenzionalmente, con l'intento di commettere un falso; l'immissione, l'alterazione, la cancellazione e/o la soppressione di dati informatici e/o programmi informatici, o altre interferenze con sistemi informatici, fatte intenzionalmente con l'intento di ostacolare il funzionamento di un sistema informatico e/o di telecomunicazione e l'accesso o l'intercettazione di un sistema informatico e/o telematico effettuato consapevolmente e senza l'autorizzazione del responsabile del sistema, violando le misure di sicurezza o con qualsiasi altro intento disonesto o dannoso).

A valle di un passaggio intermedio attraverso la nozione di *computer-related crimes* che cominciava a prendere timidamente le mosse dalla definizione "con ancoraggio fisico" dei reati commessi in ambiente digitale[19], la più coraggiosa concettualizzazione dei modelli di incriminazione del *cybercrime* può essere individuata in una tripartizione, frequentemente riferita al crimine organizzato ma generalizzabile anche a forme di reato non plurisoggettivo. Si tratta della fortunata triade *cyber-dependent, cyber-enabled* e *cyber-assisted*

15. Bricola 1978.
16. Delogu 1974, p. 19 ss.
17. Sulla natura "programmatica" della tutela penale a partire dai suoi principi fondamentali v. De Francesco 2004, p. 62 ss.
18. OECD 1986.
19. European Committee on Crime Problems 1990.

crimes elaborata dalla dottrina criminologica[20] ma di grande efficacia euristica anche ai fini dell'analisi delle trasformazioni indotte dalla transizione digitale nelle categorie concettuali del diritto penale e nei relativi modelli di incriminazione. In una sorta di progressione discendente in termini di connessione funzionale con l'ambientamento digitale si distinguono, infatti, (i) attività criminose che sono *create/rese possibili* dalle nuove tecnologie informatiche e che, per riprendere – pur in termini rovesciati – l'immagine del gemellaggio prima menzionata, non hanno un *analog twin* (come nel caso degli attacchi *ransomware* ad una infrastruttura critica), (ii) attività criminose che risultano variamente potenziate dal ricorso alle tecnologie informatiche (si tratta del caso, tra gli altri, dei reati a mezzo stampa commessi nell'ambito di social network) e che hanno una sorta di *analog twin* pur più debole e contenuto e (iii) reati che sono, per così dire, già conosciuti nel mondo fisico (si pensi al caso, ampiamente presente nella prassi giurisprudenziale, delle truffe *on line*) ma che, tra le diverse modalità di realizzazione, sono compatibili anche con quella *cyber* e ove l'immagine dell'*analog twin* dovrebbe essere la più pertinente, in quanto riferita, quantomeno nella logica della predetta concettualizzazione categoriale, allo *stesso* reato ma commesso *on line*.

In verità, a ben vedere tale tripartizione tende a perpetuare l'anelasticità e l'antropomorfismo di un diritto penale refrattario ai cambiamenti indotti dalla tecnologia in quanto, pur nell'accezione negativa della ricordata mancanza di un corrispondente gemello analogico, tende a rappresentare il cybercrime come una sorta di anomalia del sistema penale a cui quest'ultimo deve faticosamente adattarsi opponendo al cambiamento, almeno fin dove possibile, un modello speculare tradizionale in tal modo istituendo anche una sorta di ideale, o forse, cripto-progressione ascendente dell'impatto della transizione digitale su principi e regole del diritto penale dal minimo della categoria (iii) al massimo della categoria (i).

Posto che, tuttavia, come ricordato il fondamento di garanzia dei principi cardine del sistema penale debba sfuggire tanto ad una logica antropomorfica quanto all'anelasticità rispetto ai cambiamenti indotti dalla transizione digitale, non parrebbe, invero, contestabile che i principi fondazionali del sistema (a partire da quello di legalità) debbano trovare ugualmente applicazione quale che sia la subcategoria di *cybercrime* e forse proprio *a fortiori* nelle ipotesi che si sono definite *cyber-dependent* nel nome di quella storicità[21] dei diritti – e delle relative garanzie – che ne costituisce contenuto essenziale e che, come tale, si oppone ad approcci conservativi ed anelastici come anche ad attenuazione delle garanzie a fronte di inedite forme di criminalità smaterializzata.

Spostandosi, invece, dal livello dei principi fondamentali a quello dei modelli di incriminazione, la tripartizione, pur di grande e perdurante valore euristico e classificatorio, sopra menzionata presenta, dal versante delle trasformazioni delle categorie di diritto penale sostanziale, taluni profili meritevoli di valutazione critica. Sembrerebbe, infatti di poterne inferire una diversa gradazione della *vexata quaestio* del dibattito[22] tra "eccezionalisti" e "non eccezionalisti" nell'analisi del rapporto tra diritto e transizione digitale e, per quello che attiene alla presente indagine, tra diritto penale tradizionale e cybercrime. Mentre, infatti, parrebbe prevalere una logica non eccezionalista ma di rapporto, per così dire, da *genus* a *species* rispetto alle categorie dei *cyber-enabled* e dei *cyber-assisted crimes* che in questa logica sarebbero diverse forme di manifestazione modali o strumentali di fattispecie incriminatrici già note, l'approccio alla categoria dei *cyber-dependent crime* sarebbe dominata da una prevalente logica eccezionalista di un orizzonte di incriminazione totalmente inedito e al limite dell'anomalia in un sistema fondato sulla (indimostrata, indimostrabile e storicamente smentita) necessità che il modello-standard di crimine sia solo quello commesso nel mondo fisico-analogico. Un tale ragionamento paralogistico in quanto basato sulla premessa erronea che i

20. Wall 2004-a, p. 20 ss.; Wall 2004-b, p. 309 ss., McGuire–Dowling 2013, Di Nicola 2022, Di Nicola 2021.

21. "Perché i diritti dell'uomo, per fondamentali che siano, sono diritti storici, cioè nati in certe circostanze, contrassegnate da lotte per la difesa di nuove libertà contro vecchi poteri, gradualmente, non tutti in una volta e non una volta per sempre", Bobbio 1990, p. 7.

22. Goldsmith 1999; Johnson–Post 1996.

modelli di incriminazione siano anelastici rispetto alle trasformazioni digitali e che, in mancanza di un *analog twin*, il modello di incriminazione del *cyber-dependent crime* abbia una portata eccezionale rispetto al sistema potrebbe porre le premesse per un'inaccettabile impostazione da doppio standard anche rispetto all'operatività dei principi fondamentali, rigidamente applicabili, in analogia ai modelli tradizionali di incriminazione, ai *cyber-enabled* e *cyber-assisted crimes*, e, invece, più sfumati con riguardo ai *cyber-dependent crime*.

Nella richiamata ottica di una specularità tra transizione digitale e transizione dei modelli giuridico-penali di riferimento per l'incriminazione dei reati commessi in ambiente digitale, parrebbe, piuttosto, doversi ritenere che tutti i *cybercrimes* siano, *by definition, cyber-dependent* necessitando di una rifondazione *ab imis* di programmi e modelli delle incriminazioni che, pur con diversi riferimenti categoriali, permettano di valorizzare le funzioni del diritto penale nel più ampio quadro della prevenzione e del contrasto al reato commesso in ambiente digitale.

3. Verso nuovi paradigmi di diritto penale sostanziale *by cyber-design*

Nella ricordata ottica della proposta di un nuovo volto del diritto penale di fronte alla transizione digitale in una prospettiva autonomistica e non analogica si pone la necessità di valorizzare i tratti comuni di tutte le forme di *cybercrime* andando oltre la tripartizione dei modelli di incriminazione. In particolare, si tratta di valutare la fattibilità di un'evoluzione della definizione del modello di incriminazione delle condotte poste in essere in contesto digitale oltre il *paradigma analogico* che sfrutta le fattispecie esistenti adattandole alla variante digitale e il *paradigma strumentale* che fa leva sul mezzo informatico per costruire fattispecie modellate tenendo conto degli effetti del ricorso allo strumento informatico. Si pensi al noto esempio del domicilio informatico per concettualizzare i modelli di incriminazione dell'accesso abusivo e che ha indotto a collocare nella sezione relativa ai *delitti contro l'inviolabilità del domicilio* le fattispecie di cui agli artt. 615-*ter* c.p. (*Accesso abusivo ad un sistema informatico o telematico*), 615-*quater* c.p. (*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*), e 615-*quinquies* c.p. (*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*), tutte trainate dalla fattispecie generale di "Violazione di domicilio" ma punite – almeno avuto riguardo alla pena-base – meno gravemente rispetto alle analoghe fattispecie relative al "domicilio fisico". Si ponga altresì mente al binomio dato/cosa mobile ai fini dell'applicazione dei delitti contro il patrimonio, dall'appropriazione indebita al furto, allo scopo di sussumere in un fatto tipico "noto" la condotta di chi, a seguito di un accesso abusivo, si appropri di informazioni presenti nel database violato[23] e rispetto alle quali si postuli un valore economico.

L'assunto, logicamente connesso al binomio *cyber-enabled* e *cyber-assisted crime*s, secondo il quale si tratterebbe di *mere varianti* dell'analogo gemello tradizionale appare, tuttavia, revocabile in dubbio come direttamente dimostrato dagli equilibrismi interpretativi cui la giurisprudenza è frequentemente chiamata. Che l'accesso abusivo a sistema informatico presenti la stessa struttura dell'abuso di domicilio con l'unica variante del mezzo informatico appare fortemente criticabile. Radicalmente diversi risultano, infatti, il *soggetto attivo*, potenzialmente anche non corrispondente ad una persona fisica nei casi in cui tali forme di criminalità siano completamente automatizzate, il complesso degli *elementi normativi* referenti dei presupposti di legittimità dell'accesso, talvolta anche extragiuridici come, ad esempio, nel caso dell'utilizzo di strumenti crittografici, *modus* e *tempus commissi delicti* che, nella sfera dei *cybercrimes*, possono sensibilmente variare e contrarsi rispetto al mondo fisico-analogico rispetto alla persona offesa, che, anche nei reati a vittimizzazione individuale, risulta comunque connotata da una prospettiva, *lato sensu*, esponenziale in ragione della

23. In giurisprudenza *ex multis* v. Cass. Pen., sez. II, 18 febbraio 2016, n. 21596, in "Il penalista.it", 22 giugno 2016. Cfr. anche Cass. pen., sez. II, 7 novembre 2019, n.11959, in "dejure.it.", che sottolinea che si fa espressamente riferimento all'esigenza "di interpretare talune categorie giuridiche che, coniate in epoche in cui erano del tutto sconosciute le attuali tecnologie informatiche, devono necessariamente esser nuovamente considerate". Per una lettura critica v. Pisani 2020.

ripetibilità delle condotte e della loro scalabilità, mediata dalla tecnologia, verso numeri massivi di soggetti passivi. Si pensi, a tale ultimo proposito, agli effetti delle pratiche di *social engineering* sull'emersione di nuove vulnerabilità anche determinate dall'inattitudine della previa vittimizzazione da *cybercrime* ad aumentare la consapevolezza e la percezione del rischio[24]. In questi casi, la vittima, pur formalmente "singola" non è soltanto individuale, alla stregua del classico binomio individuale-collettivo del diritto penale tradizionale, ma è un target esposto a condotte penalmente rilevanti in quanto espressivo di caratteristiche riferibili ad un ampio gruppo che abilita soggetti, e spesso perfino gruppi criminali, alla commissione seriale di reati che, *mutatis mutandis*, possono comunque definirsi "a vittimizzazione collettiva non sincrona".

La profonda diversità dei *cybercrimes as such* rispetto al fondamento giustificativo dei modelli tradizionali di incriminazione, dunque, suggerisce di convergere su paradigmi autonomistici di *cybercrime by design* ove la fattispecie incriminatrice non costituisca la variante di un modello già conosciuto ma integri *ab initio* un illecito, non necessariamente penale, interamente calibrato sul contesto digitale del suo autore, della condotta e di tutti gli elementi costitutivi del reato. L'insidia da evitare nella costruzione di un modello di cybercrime che si è voluto definire *by design* è costituita dall'abuso della generalizzazione del modello, per rifarsi alla tripartizione sopra menzionata, del *cyber-dependent crime* e ove il piano del rispetto dei principi venga rarefatto a fronte di un modello di incriminazione altrettanto "smaterializzato" con la conseguenza che si possa, per così dire, tollerare, un affievolimento del vincolo alla tassatività e determinatezza della fattispecie in nome dell'efficienza dell'intervento penalistico, talvolta anche emergenziale e privo di una visione di sistema, a presidio degli interessi protetti.

Singolarmente paradigmatica di tale insidia è la fattispecie di pornografia virtuale di cui all'art. 600-*quater*.1 c.p. la quale estende l'applicazione delle disposizioni aventi ad oggetto la pornografia minorile (art. 600-*ter* c.p.) e la detenzione ed accesso a materiale pornografico (art.600-*quater* c.p.) anche ad immagini virtuali che potrebbero essere state realizzate con tecniche di elaborazione grafica non associate ad immagini reali ma la cui qualità di rappresentazione le faccia apparire come vere situazioni. Come ampiamente rilevato dalla dottrina[25], si tratta di forme di criminalizzazione ove l'esclusivo ambientamento virtuale può condurre ad una grave compromissione di principi fondamentali in quanto volta a stigmatizzare condotte espressive di un "tipo d'autore" e non di una condotta offensiva di beni giuridici meritevoli di tutela con scopi di moralizzazione che dovrebbero rimanere estranei ad un diritto penale laico. Sotto tale angolo visuale, la prospettiva autonomistica dei modelli di incriminazione del *cybercrime* e l'attribuzione allo stesso di una dignità autonoma dall'essere la variante di un corrispondente modello analogico può innanzi tutto contribuire, ribadita la necessità del rispetto dei principi fondamentali, a sottoporre le scelte di criminalizzazione ad un efficace e, in sede di *drafting* legislativo, preliminare *subsidiarity test* in ordine alla conformità con il principio di frammentarietà ed *extrema ratio* del diritto penale della stessa scelta dello strumento criminale per punire una condotta realizzata in ambiente digitale.

A tal riguardo il raffronto tra il reato di pornografia virtuale e la strategia legislativa a prevenzione e contrasto del *cyberbullismo* di cui alla legge 71/2017 può risultare, ai fini che qui interessano, particolarmente promettente in quanto espressivo di un ricorso simbolico e stigmatizzante del diritto penale non direttamente connesso ad adeguate azioni di efficace contrasto (la pornografia virtuale) e di un (più condivisibile) intervento che,

24. Albladi–Weir 2020, p. 4.

25. V. Delsignore 2023, p.388 ss. Sullo specifico punto della compatibilità con i principi fondamentali dell'uso del diritto penale per punire comportamenti posti in essere in modalità integralmente digitale v. anche Maugeri 2021, Maugeri 2020, p. 908 ss., con riferimento alle fattispecie di cui agli artt. 600-*quater* c.p. e 600-*quater*.1 c.p., rispettivamente considerate un esempio "paradigmatico" e un esempio "esasperato" del diritto penale "del nemico" *in subiecta materia*, con evidente anticipazione della soglia dell'intervento penale, a sanzionare comportamenti piuttosto sintomatici di un particolare "tipo di autore" che non direttamente lesivi del bene giuridico da tutelare. *Amplius* la compiuta analisi di Fiorinelli 2024, p. 110 ss.

al contrario, non viene affidato allo strumento criminale ma ad una diversa politica di prevenzione e contrasto basata sulla responsabilizzazione del gestore del sito Internet e la previsione di interventi immediati di blocco e rimozione dei contenuti on line, ferma restando la configurabilità di gravi reati, quali, ad esempio, quello di atti persecutori di cui all'art. 612-*bis* c.p., qualora ne ricorrano tutti gli elementi costitutivi. Come sostenuto dalla dottrina[26], si tratta di un approccio da valutare positivamente in ragione della sinergia tra strumenti penali e rimediali "attivabili anche al di fuori del (più impervio) percorso processual-penalistico di accertamento del fatto" facendo "ricorso a poteri coercitivi per l'eliminazione delle 'conseguenze' del reato, non più da intendersi quale adempimento posto programmaticamente a carico dell'autore dell'illecito" da parte dell'autorità di law enforcement "ma anzi quale obiettivo *primario* perseguito dal legislatore, nell'ambito di un paradigma di prevenzione *in concreto*".

Laddove, invece, il *subsidiarity test* della meritevolezza di sanzione penale della condotta illecita posta in essere in contesto digitale venga superato e, nel rispetto del principio di frammentarietà, si proceda all'introduzione nel sistema di una fattispecie incriminatrice, l'approccio autonomistico potrebbe fondare tecniche di legislazione penale, per l'appunto, *by design* in quanto non volte ad appiattire il cybercrime sul "gemello analogico" ma a costruire reati calibrati sul peculiare modo d'essere della criminalità *on line*.

Pur con tutte le riserve legate alla prossimità temporale dell'intervento e alla necessità della formazione di una più consistente giurisprudenza di merito e di legittimità, un interessante modello di riferimento di forme autonome di cybercrime *by design* può essere tratto dall'ambito della *cybersecurity* dalle strategie nazionali ed internazionali al recente intervento di cui alla legge 28 giugno 2024, n. 90, la quale impone quel "riassestamento assiologico"[27] delle diverse forme di manifestazione di una criminalità che, in ragione della pervasività dei suoi effetti offensivi, sfugge ad una lettura riduzionistica ad una variante virtuale dei reati contro la sicurezza pubblica tradizionalmente intesa o, come ricordato, della criminalità contro il patrimonio per finalità di profitto. Dalle estorsioni informatiche alla coercizione digitale, dalle varie forme di attentato alle infrastrutture critiche alla progressiva emersione di nuove forme di criminalità organizzata digitale anche con accenti di *crime-as-a-service*, la criminalizzazione degli attacchi alla cybersicurezza si iscrive in un sistema ove la fattispecie incriminatrice non è più un elemento *standalone* ma si colloca all'interno di una più ampia strategia di prevenzione, contrasto e *rapid-reaction* che ruota intorno al volano della notifica degli incidenti al fine della realizzazione degli interventi immediati di reazione e contribuisce ulteriormente alla transizione verso un modello autonomistico ed integrato di intervento penale che, superato il *subsidiarity test*, possa assumere una marcata connotazione *multistakeholder* e collaborativa in una logica di partenariato esteso nella definizione delle politiche di contrasto alla cybercriminalità.

Alla medesima logica che si è voluta definire "autonomistica" può essere ricondotta anche la legge 23 settembre 2025, n. 132 avente ad oggetto *Disposizioni e deleghe al Governo in materia di intelligenza artificiale* la quale, al di là dell'apparente assonanza con modelli di incriminazione e circostanziali già conosciuti, affronta il tema dell'intersezione tra diffusione dell'intelligenza artificiale e criminalità in una prospettiva di sistema e non emergenziale e analogica. Alla predetta *ratio* politico-criminale sembrerebbero potersi, in particolare, ascrivere l'art. 612-*quater* c.p. (*Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale*) che punisce con la reclusione da uno a cinque anni chiunque cagiona un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità, o l'art. 294 (*Attentati contro i diritti politici del cittadino*) che punisce con la reclusione da due a sei anni l'inganno posto in essere mediante l'impiego di sistemi di intelligenza artificiale o, in termini ancora più generali l'art. 61 n. 11-*decies* c.p., ai sensi del quale viene introdotta una nuova aggravante comune consistente ne "l'avere commesso il fatto mediante l'impiego di sistemi

26. Fiorinelli 2024, p. 129.

27. *Ivi*, p. 146.

di intelligenza artificiale, quando gli stessi, per la loro natura o per le modalità di utilizzo, abbiano costituito mezzo insidioso, ovvero quando il loro impiego abbia comunque ostacolato la pubblica o la privata difesa, ovvero aggravato le conseguenze del reato". Il carattere sistematico dell'intervento coinvolge anche ipotesi di reati economici come l'aggiotaggio di cui all'articolo 2637 del codice civile che punisce con la reclusione da due a sette anni il fatto commesso mediante l'impiego di sistemi di intelligenza artificiale e il *market abuse* di cui all'articolo 185, comma 1, del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, analogamente punito con pene molto elevate qualora commesso mediante l'impiego di sistemi di intelligenza artificiale.

Nella prospettiva, antica ma autenticamente visionaria, della consapevolezza dell'effetto trasformativo del medium del reato sulle categorie della teoria generale del reato, la transizione digitale suggerisce, come lo "strumento" nella riflessione di Tullio Delogu, una transizione verso una nuova postura del diritto penale nel sistema di prevenzione e contrasto della criminalità in ambiente digitale che, in una prospettiva integrata, sia idealmente disposta, come nella *success story* del cyberbullismo, a rinunciare ad una funzione inutilmente simbolica a favore di un più efficace sistema di gestione del rischio e di contrasto dell'illecito. In questa prospettiva, e ben al di là del disegno del modello di incriminazione, una legislazione, anche penale, *by cyber-design* non può non fondarsi su un paradigma di responsabilizzazione condivisa ove ciascuno, a partire dalla vittima dell'illecito, si faccia "garante di prossimità" e cooperi, anche *praeter delictum*, alla prevenzione, alla repressione e alla riparazione delle conseguenze del *cybercrime*.

4. La trasformazione dei modelli di law enforcement dalla repressione *ex post* alla prevenzione cooperativa

La transizione verso nuove ed autonome forme di intervento del diritto penale di fronte alla criminalità in ambiente digitale porta con sé una trasformazione dei modelli di law enforcement il cui tratto, tra i molti, maggiormente distintivo è costituito dalla socializzazione o dalla solidarietà nella gestione del rischio-reato nel *cyberspace*. Nel solco della teorica dei reati omissivi impropri e della posizione di garanzia rispetto alla tutela di beni giuridici meritevoli di tutela (anche) penale, l'impatto della rivoluzione tecnologica sulla moltiplicazione dei predetti garanti ha un volto anch'esso "antico" in quanto riferibile all'ampio dibattito teorico, giurisprudenziale e regolatorio sullo statuto della responsabilità dei *digital service providers*. Pur non essendo questa la sede per trattare *funditus* il tema, la responsabilizzazione del provider rispetto agli illeciti commessi dagli utenti dei servizi messi a disposizione rimanda alla nozione sopra menzionata di "garante di prossimità". A fronte delle indubbie difficoltà di accertamento degli illeciti commessi on line, elevare il provider ad una posizione di controllo risulta senz'altro pertinente rispetto alle questioni problematiche del law enforcement nel *cyberspace*. Al di là dell'adesione al modello della caratterizzazione commissiva o omissiva della sua responsabilità, l'elemento di maggiore rilievo nell'ottica della transizione dei modelli di law enforcement è costituito dall'attitudine del provider a svolgere un *continous monitoring* idoneo ad andare oltre la prospettiva tradizionale, e puntuale-episodica, dell'obbligo giuridico di impedimento del singolo reato altrui.

Invero, il dibattito sullo statuto giuridico della responsabilità del provider e sull'ampiezza della sua posizione di garanzia è stato prevalentemente dominato dall'inquietante spettro della criminalizzazione del mancato controllo o del mancato impedimento. Pur a fronte della limpida teorica[28] della simmetria tra poteri di intervento e obblighi di monitorare, di attivarsi per denunciare/segnalare o di impedire, la giurisprudenza ha progressivamente condotto il predetto statuto della responsabilità del provider dal minimale dovere di attivarsi in presenza della conoscenza di fatti illeciti al dovere generalizzato di impedimento del reato commesso in rete dal suo utente sulla scorta, per l'appunto, della *prossimità* del provider ad una fonte di rischio e ad illeciti difficili da accertare da parte della autorità pubblica di law enforcement.

Alla base della predetta estensione dei doveri impeditivi del *digital service provider* parrebbe, tuttavia, prevalere, per un verso, una logica monopolistica in capo all'autorità pubblica del

28. Fondamentale in argomento la riflessione di Leoncini 1999, p. 55 ss.

law enforcement che si traduce poi in una cripto-delega al garante prossimo per il tramite della panpenalizzazione della violazione dei suoi doveri di intervento (ed impedimento) *post factum*. Parrebbe, tuttavia, ancora una volta trattarsi di una soluzione "analogica" della questione problematica del law enforcement nel *cyberspace* operata attraverso il ricorso a categorie tradizionali, quali, per l'appunto, gli (estesi) obblighi di impedimento e le (dilaganti) diverse forme di responsabilità penale omissiva propria ed impropria.

In linea con l'approccio autonomistico alla trasformazione dei modelli di incriminazione indotti dalla transizione digitale, parrebbe invece opportuno valutare di postulare nell'ampia categoria che si è voluta definire dei "garanti prossimi" lo sviluppo di forme di *cooperative compliance praeter delictum* ove i doveri di collaborazione prescindono dal temuto paradigma del concorso per omissione del titolare della posizione di garanzia ma si collocano nel solco di un diverso costrutto dialogico tra "garanti (privati) di prossimità" e autorità (pubbliche) di law enforcement[29]. Dal binomio classico potere/responsabilità penale potrebbe, dunque, ipotizzarsi una più promettente scissione concettuale ove il potere (di monitoraggio ed intervento) sia finalizzato ad evitare l'imputazione di responsabilità (anche penali) valorizzando il volto difensivo e non ascrittivo del potere. Tale paradigma estensivo dei doveri di controllo sull'integrità del contesto digitale gestito dal provider costituisce, invero, la premessa concettuale per un cambio di paradigma anche nella prospettiva vittimologica. Attraverso un processo assimilabile, pur *mutatis mutandis*, a quello ravvisabile nel diritto penale del lavoro, l'impossibilità di limitare il monitoraggio al singolo fatto illecito commesso in rete porta con sé la "discesa" della responsabilizzazione fino agli *end users, rectius* gli utenti e, agli effetti della legge penale, dei titolari dei beni giuridici protetti che, analogamente ad altri ambiti del diritto penale dell'economia, si allontanano sempre più dal modello del creditore passivo, e a tratti inconsapevole, di protezione per divenire sempre più vicini alla nozione di co-obbligati alla (auto) tutela con tutto il corredo di *awareness, resilience* e *solidarity* che costituiscono la più moderna e internazionalmente condivisa declinazione di *cybersecurity*.

5. Prolegomeni del nuovo volto del diritto penale del *cyberspace*

In conclusione dell'analisi dell'impatto della transizione digitale sui modelli di incriminazione ed i percorsi di law enforcement, è proprio nel passaggio dal modello analogico e, a tratti, insidiosamente metaforico di soluzioni mutuate da ambiti tradizionali a quello che si è voluto definire autonomistico che parrebbe potersi individuare il nuovo volto del diritto penale del *cyberspace*. Al di là di logiche emergenziali che spesso collassano in forme di panpenalizzazione e incriminazione simbolica di illeciti che suscitano particolare allarme sociale, un rigoroso filtro di frammentarietà impone di riservare, anche e soprattutto nella dimensione digitale, al diritto penale il contrasto dei più gravi illeciti che offendano diritti fondamentali in una prospettiva ove il diritto penale non sia la *prima ratio* ma un elemento di un sistema integrato composto anche da misure preventive, rimediali, civili o amministrative e ove tra modelli di incriminazione e paradigmi di law enforcement vi sia una sinergia concettuale ed assiologica[30].

La necessità di approcci autonomistici alla definizione dei modelli di incriminazione nel *cyberspace* consente di rivalutare criticamente le classiche tripartizioni dei *cybercrimes* sulla base del crescente livello di analogia con fattispecie incriminatrici tradizionali come anche di rivedere la distinzione tra reati a vittimizzazione individuale e collettiva. Pur conservando anche questo binomio una sua validità classificatoria e politico-criminale, la pervasività del contesto digitale in diritto penale attribuisce alla vittima individuale un significato "esponenziale" e "scalabile" che trascende dalla nozione "fisico-analogica" della vittimizzazione singola potendo, peraltro, innescare

29. Pur trattandosi di una categoria sviluppata prevalentemente negli studi economico-manageriali e, in ambito giuridico, nel settore del diritto tributario (Björklund Larsen–Oats 2019, p. 165 e Troiano 2017/2024, p.10), la categoria della *cooperative compliance* può risultare molto pertinente, combinata alle più recenti evoluzioni della nozione di cyber resilienza, all'evoluzione dei modelli di law enforcement pubblico-privato nel *cyberspace*.

30. In argomento McGuire 2017, p. 35 ss.

processi di vittimizzazione a catena che presentano una nuova dimensione della collettività rispetto alle tradizionali definizione della sicurezza pubblica o collettiva.

Una concettualizzazione autonomistica dei modelli di incriminazione e di law enforcement presenta altresì il vantaggio di suggerire approcci "scalabili" anche in altri ambiti che con quello della transizione digitale condividano la stessa necessità di elasticità in presenza di cambiamenti "totalizzanti" quali, tra gli altri, quelli indotti dal cambiamento climatico, o dai rischi CBRN o dal sempre crescente impiego delle tecnologie robotiche nella produzione, nel lavoro, nella sanità.

Ribadito il principio di *extrema ratio*, il nuovo volto del diritto penale può disvelare le sue potenzialità preventive e cooperative non tanto e non solo in funzione di imputazione della responsabilità *post delictum* ma di prevenzione e organizzazione nella gestione del rischio *ante* e *praeter delictum* in una più moderna declinazione della prevenzione generale positiva che faccia prevalere su quello simbolico il profilo più solidaristico e collaborativo del contrasto (anche penale) alla cybercriminalità.

Riferimenti bibliografici

S.M. Albladi, G.R.S. Weir (2020), *Predicting individuals' vulnerability to social engineering in social networks*, in "Cybersecurity", vol. 3, 2020, n. 1

U. Beck (2000), *La società del rischio. Verso una seconda modernità,* trad. it., Carocci, 2000

L. Björklund Larsen, L. Oats (2019), *Taxing Large Businesses: Cooperative Compliance in Action*, in "Inter economics", vol. 54, 2019, n. 3

N. Bobbio (1990), *L'età dei diritti*, Einaudi, 1990

R. Bodei (2019), *Dominio e sottomissione. Schiavi, animali, macchine, intelligenza artificiale*, Il Mulino, 2019

F. Bricola (1978), *Responsabilità penale per il tipo e per il modo di produzione*, in Aa.Vv., "La responsabilità dell'impresa per i danni all'ambiente e ai consumatori", Giuffrè, 1978

B.C. Cheong (2022), *Avatars in the Metaverse: Potential Legal Issues and Remedies*, in "International Cybersecurity Law Review", vol. 3, 2022

G.A. De Francesco (2004), *Programmi di tutela e ruolo dell'intervento penale*, Giappichelli, 2004

T. Delogu (1974), *Lo "strumento" nella teoria generale del reato*, in "Rivista italiana di diritto e procedura penale", 1974

V. S. Delsignore (2023), *La tutela dei minori e la pedopornografia telematica: i reati dell'art. 600-ter c.p.*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (diretto da), "Trattato di diritto penale – Cybercrime", Utet giuridica, 2023

A. Di Nicola (2022), *Towards digital organised crime and digital sociology of organised crime*, in "Trends in organised crime", 2022

A. Di Nicola (2021), *Criminalità e criminologia nella società digitale*, FrancoAngeli, 2021

European Committee on Crime Problems (1990), *Computer-related crime*, Council of Europe Publishing and Documentation Services, 1990

G. Fiorinelli (2024), *La violenza mediata dalla tecnologia. Dogmatica, profili politico-criminali e interpretazione della nozione di violenza nel diritto penale delle tecnologie digitali*, Giappichelli, 2024

T.E. Frosini (2020), *Il Costituzionalismo nella Società tecnologica*, in Aa.Vv., "Liber amicorum per Pasquale Costanzo", in Consulta Online, 2020

V. Frosini (2000), *L'orizzonte giuridico dell'Internet*, in "Il Diritto dell'informazione e dell'informatica", 2000, n. 2

A. Garapon, J. Lassegue (2021), *La giustizia digitale. Determinismo tecnologico e libertà*, trad. it, Il Mulino, 2021

A. Gargani (2019), *Jus in latenti. Profili di incertezza del diritto penale dell'ambiente*, in "Criminalia. Annuario di scienze penalistiche", 2019

J.L. Goldsmith (1999), *Against Cyberanarchy*, University of Chicago Law Occasional Paper, n. 40, 1999

E. Haber (2024), *The Criminal Metaverse*, in "Indiana Law Journal", 2024, n. 99

W. Hoffmann-Riem (2020), *Digitale Disruption und Transformation. Herausforderungen für Recht und Rechtswissenschaft*, in M. Eifert (Hrsg.), "Digitale Disruption und Recht", Nomos, 2020

A. Iannuzzi (2024), *Metaverso, Ditigal Twins e diritti fondamentali*, in "Rivista italiana di informatica e diritto", 2024

A. Iannuzzi, F. Laviola (2023), *I diritti fondamentali nella transizione digitale tra libertà e uguaglianza*, in "Diritto costituzionale", 2023, n. 1

A. Incampo (2025), *Come del mondo (o del diritto o dell'economia) fin dalla sua origine*, in "Rivista di Filosofia del diritto", 2025, n. 1

R. Johnson, D. Post (1996), *Law and Borders – The Rise of Law in Cyberspace*, in "Stanford Law Review", 1996

I. Leoncini (1999), *Obbligo di attivarsi, obbligo di garanzia e obbligo di sorveglianza*, Giappichelli, 1999

E. Longo (2023), *Giustizia digitale e Costituzione. Riflessioni sulla trasformazione tecnica della funzione giurisdizionale*, FrancoAngeli, 2023

A.M. Maugeri (2021), *I reati sessualmente connotati e diritto penale del nemico*, Pisa University Press, 2021

A.M. Maugeri (2020), *I reati sessualmente connotati e diritto penale del nemico*, in "Rivista italiana di diritto e procedura penale", 2020

M.R. McGuire (2017), *Technology crime and technology control*, in M.R. McGuire, T.J. Holt (eds.), "The Routledge Handbook of Technology, Crime and Justice", Routledge, 2017

M.R. McGuire (2012), *Technology, Crime and Justice. The question concerning technomia*, Routledge, 2012

M.R. McGuire, S. Dowling (2013), *Cybercrime: a review of the evidence*, Home Office Research report 75, October 2013

OECD (1986), *Computer related crime: analysis of legal policy*, OECD Publishing, 1986

T. Padovani (1996), *Il nuovo volto del diritto penale del lavoro*, in "Rivista trimestrale di diritto penale dell'economia", 1996

N. Pisani (2020), *La nozione di "cosa mobile" agli effetti penali e i file informatici: il significato letterale come argine all'applicazione analogica delle norme penali*, in "Diritto penale e processo", 2020

R. Razzante (2022), *L'attribuzione degli attacchi informatici*, in "European Journal of Pricacy Law and Technologies", 2022

G.M. Riccio (2023), *Metaverso, logiche proprietarie e poteri privati*, in G. Cassano, G. Scorza, "Metaverso. Diritti degli utenti – piattaforme digitali – privacy – diritto d'autore – profili penali – blockchain e NFT", Pacini Giuridica, 2023

G. Sartor (2017), *Human Rights and Information Technologies*, in R. Brownsword, E. Scotford, K. Yeung (Eds.), "The Oxford Handbook of Law, Regulation and Technology", OUP, 2017

F. Sarzana di Sant'Ippolito, M.G. Pierro, I.O. Epicoco (2022), *Il diritto del metaverso. NFT, DeFi, GameFi e privacy*, Giappichelli, 2022

G. Sciancalepore (2023), *Intelligenza artificiale, metaverso e diritto*, in "Iura & Legal systems", 2023

C.J. Smith (2004), *Research on crime and technology*, in E.U. Savona (ed.) "Crime and Technology", Springer, 2004

L. Stortoni (2004), *Angoscia tecnologica ed esorcismo penale*, in "Rivista italiana di diritto e procedura penale", 2004

U. Troiano (2017/2024), *Intergovernmental Cooperation and Tax Enforcement*, National Bureau of Economic Research Working Paper 2017 (revised December 2024)

D.S. Wall (2004-a), *What are Cybercrimes?*, in "Criminal Justice Matters", vol. 58, 2004, n. 1

D.S. Wall (2004-b), *Digital realism and the governance of spam as cybercrime*, in "European Journal on Criminal Policy and Research", 2004

Sezione monografica

Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement

Indagini criminologiche, diritto penale, diritto internazionale

a cura di

Gaetana Morgante e Gaia Fiorinelli

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0255 • articolo sottoposto a peer review • pubblicato in anteprima il 22 dic. 2025

Gaia Fiorinelli

La recente "disciplina penale" del *cybercrime* tra armonizzazione internazionale e interventi nazionali: convergenze parallele?

La tutela penale del cyberspazio è stata, per lungo tempo, il terreno privilegiato di una politica criminale quasi esclusivamente "armonizzata" a livello internazionale ed europeo. Negli ultimi anni, tuttavia, emergono due tendenze divergenti. Da un lato, nella dimensione globale si registra una rilevante evoluzione con l'adozione della Convenzione ONU contro il Cybercrime (2024) e la *Draft Policy on Cyber-Enabled Crimes* (2025) dell'Ufficio del Procuratore della Corte Penale Internazionale, che qualificano il cybercrime come una minaccia rilevante nell'interesse dell'intera comunità internazionale. Dall'altro lato, si moltiplicano in questa materia le iniziative unilaterali dei legislatori statali, soprattutto in aree percepite come strategiche per la sicurezza e l'interesse nazionale (ad esempio, attacchi *ransomware*, FIMI, disinformazione). La ricerca analizza criticamente questa sovrapposizione di interventi penalistici, assumendo il concetto di (cyber)sicurezza come prisma interpretativo che scompone – ma al tempo stesso connette – la politica criminale in materia di *cybercrime*, tra equilibrio geopolitico globale e tutela della sicurezza nazionale.

Cybercrime – Cybersicurezza – Diritto penale – Armonizzazione – Sicurezza nazionale

The emerging criminal law framework on cybercrime between international harmonization and domestic interventions: Parallel convergences?

The criminal-law protection of cyberspace has long been the privileged domain of a criminal policy that was almost exclusively "harmonized" at the international and European levels. In recent years, however, two diverging trends have emerged. On one hand, the global dimension has seen further developments with the adoption of the UN Convention against Cybercrime (2024) and the Draft Policy on Cyber-Enabled Crimes released by the Office of the Prosecutor of the International Criminal Court (2025), which classify cybercrime as a significant threat to the interests of the international community as a whole. On the other hand, unilateral initiatives by national legislators have multiplied in this field, particularly in areas perceived as strategic for security and national interests (e.g., ransomware attacks, FIMI, disinformation). This research critically examines the overlapping layers of criminal-law interventions, using the concept of (cyber)security as an interpretive lens that both breaks down – and at the same time connects – criminal policy in the field of cybercrime, situated between global geopolitical balance and the protection of national security.

Cybercrime – Cybersecurity – Criminal law – Harmonization – National security

L'Autrice è ricercatrice TD-A in Diritto penale presso la Scuola Superiore Sant'Anna di Pisa

La ricerca si inserisce nell'ambito del Progetto PNRR "Partenariato Esteso" PE 7 SERICS Security and Rights in the Cyber Space/ Spoke 1: Progetto CybeRights Codice identificativo: M4C2 11.3 - PE0000014 - CUPJ53C22003110001

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement - Parte 1*, a cura di Gaetana Morgante e Gaia Fiorinelli

Sommario: 1. La "storia" della tutela (penale) del cyberspazio. Dall'armonizzazione internazionale ed europea all'abbandono del diritto penale. – 2. Prima traiettoria evolutiva: la riscoperta del diritto penale (globale) per la protezione della cybersicurezza. – 3. Seconda traiettoria evolutiva: *pur un linguaggio nel mondo non (più) s'usa*. L'emergere dei legislatori penali nazionali nel cyberspazio. – 4. La recente trasformazione del diritto penale italiano: dal contrasto al *cybercrime* alla tutela della cybersicurezza nazionale. – 5. Riflessioni conclusive: riconciliare *sicurezza* e *diritti* nella politica criminale multilivello del cyberspazio.

1. La "storia" della tutela (penale) del cyberspazio. Dall'armonizzazione internazionale ed europea all'abbandono del diritto penale.

Per elaborare un'analisi critica delle più recenti traiettorie evolutive della "disciplina penale" del *cybercrime*, è indispensabile ripercorrerne brevemente gli antecedenti storici e la relativa impostazione politico-criminale[1]. Al riguardo, è ben noto come la criminalità informatica rappresenti una delle prime aree nelle quali – nel contesto trans-nazionale ed europeo – si sono sperimentati i moduli dell'armonizzazione (sostanziale) e della cooperazione (procedurale) penale[2]. Anzi, per lungo tempo la tutela penale del cyberspazio è stata concepita come oggetto di una politica criminale *necessariamente* coordinata al di sopra del livello statale, in ragione della dimensione strutturalmente trans-nazionale delle tecnologie informatiche e digitali e, dunque, del relativo uso criminale[3]. Ciò è tanto vero che, nel corso degli anni, sono stati adottati ben otto trattati per il contrasto al *cybercrime*, in seno a sei diverse organizzazioni internazionali, di portata regionale[4].

Limitando l'attenzione ai soli strumenti rilevanti per l'ordinamento italiano, deve però evidenziarsi sin d'ora come i diversi interventi di armonizzazione che si sono susseguiti in questo

1. Per una prospettiva storica su questa materia, cfr. Brodowski 2021.
2. Cfr. Chiavario-Perduca 2022, p. 1, i quali sottolineano, rispetto allo sviluppo della cooperazione penale, il "peso" del "vertiginoso progresso tecnologico in certi settori di alta specializzazione, con la sua idoneità ad agevolare, tra l'altro, movimenti illeciti di capitali e ad aprire la strada a forme sempre più sofisticate di reati 'informatici'".
3. Cfr. in generale Wang 2025; Flor 2023; Spiezia 2023; Schjolberg 2008.
4. Cfr. Wang 2025, p. 236: vi rientrano il Consiglio d'Europa, la Comunità degli Stati Indipendenti (CIS); l'Organizzazione per la Cooperazione di Shanghai (SCO); la Lega araba; la Comunità economica degli Stati dell'Africa occidentale (ECOWAS); l'Unione Africana (AU).

settore siano stati contraddistinti – quantomeno in una prima fase – da un approccio ben più *pragmatico* che *assiologico* al contrasto della criminalità informatica. Con ciò si intende sottolineare, nello specifico, come l'avvicinamento delle disposizioni penali *sostanziali* sia stato generalmente concepito, in tali strumenti, come mero presupposto servente per una più efficace cooperazione *procedurale*, piuttosto che per l'effettivo perseguimento di una politica criminale comune[5]. In questo senso, si è non a caso rilevata in dottrina l'assenza di una vera e propria "azione collettiva globale" contro la cyber-criminalità e, dunque, si è discusso di un'armonizzazione "frammentata"[6].

Un approccio di questo tipo emerge, a ben vedere, già nella prima Raccomandazione OCSE del 1986[7] in materia di *computer-related crime*, la quale muove da una ricognizione delle soluzioni elaborate a livello nazionale, per concludere suggerendo l'adozione di un approccio coordinato, a livello internazionale, idoneo a consentire l'efficace funzionamento degli strumenti di cooperazione giudiziaria e scongiurare l'esistenza di "*computer crime heavens*"[8]. Analoga è anche la visione che emerge dalla Raccomandazione R(89) 9 del Consiglio di Europa[9], nella quale l'armonizzazione del diritto penale sostanziale, pur se non priva di una qualche autonomia concettuale, è direttamente strumentale all'obiettivo di facilitare la cooperazione a livello internazionale.

Un'impostazione similare contraddistingue, a ben vedere, anche la stessa Convenzione del Consiglio d'Europa sulla Criminalità informatica, firmata a Budapest nel 2001[10], la quale – nel suo Preambolo – allude appunto allo scopo primario di promuovere la cooperazione degli Stati parte nel contrasto alla criminalità informatica. Secondo quanto si legge nella Relazione esplicativa, la definizione di un *common minimum standard* nell'ambito del diritto penale sostanziale è intesa a facilitare il contrasto al *cybercrime* sia a livello nazionale che internazionale, quale presupposto per promuovere il ricorso agli strumenti della cooperazione giudiziaria e dello scambio di conoscenze e di esperienze nella trattazione dei casi[11]. Con ciò non s'intende certo negare l'importanza delle definizioni e delle disposizioni di carattere sostanziale contenute nella Convenzione: nondimeno, è noto come le differenti sensibilità dei legislatori nazionali in relazione alla criminalizzazione dei comportamenti illeciti e alla protezione dei diritti fondamentali online abbiano limitato la definizione degli obblighi sostanziali di criminalizzazione al "minimo comune denominatore" rinvenibile tra gli Stati parte, riservando alla legislazione procedurale un ben più ampio ambito applicativo[12]. In questo senso, si è discusso di un modello pragmatico di "armonizzazione flessibile"[13], che coniuga l'esigenza di uniformità con il rispetto delle peculiarità giuridiche e culturali di ogni Stato e che, come si anticipava, non può intendersi, a dispetto delle intenzioni, come una politica criminale globale di contrasto alla criminalità informatica.

Volgendo lo sguardo alla produzione legislativa dell'Unione europea in questo ambito, deve richiamarsi la norma generale di cui all'art. 83 TFUE,

5. In questa direzione, cfr. Brunhober 2022, p. 245.
6. Cfr. in questo senso Wang 2025, p. 236; Brunhober 2022, p. 244; Clough 2014, p. 730.
7. Cfr. OCSE, *Computer-related crime: analysis of legal policy*, Paris, 1986.
8. *Ivi*, p. 64 ss.
9. Cfr. Consiglio d'Europa, Comitato dei Ministri, *Raccomandazione n. R(89)9 del Comitato dei Ministri agli Stati Membri sul crimine informatico*, adottata dal Comitato dei Ministri in data 13 settembre 1989 alla 428ª riunione dei Deputati dei Ministeri, nonché European Committee on Crime Problems, *Computer-related crime*, Council of Europe Publishing and Documentation Services, 1990.
10. Cfr. Consiglio d'Europa, *Convenzione sulla criminalità informatica*, Budapest, 2001.
11. Cfr. Consiglio d'Europa, *Explanatory Report to the Convention on Cybercrime*, 2001, p. 7.
12. Cfr. in generale Clough 2014. L'ambito di applicazione delle disposizioni procedurali è individuato dall'art. 14 della Convenzione, non soltanto con riferimento alle fattispecie penali introdotte nella Sezione relativa al diritto penale sostanziale, ma anche agli altri reati commessi utilizzando tecnologie informatiche, e persino a tutti i casi nei quali sia necessaria la raccolta delle prove in formato elettronico.
13. Cfr. in questi termini Clough 2014, p. 709.

che ora funge da cornice sistematica per tutti gli interventi dell'Unione in materia penale. In essa, la "criminalità informatica" è appunto annoverata tra le materie nelle quali può esplicarsi la competenza penale dell'Unione europea, in ragione della sua intrinseca "dimensione transnazionale" e della sua "particolare gravità", nonché dell'esigenza di contrastarla "su basi comuni". Prima della vigenza di tale disposizione, già la Decisione Quadro n. 222 del 2005[14] si poneva l'obiettivo di migliorare la cooperazione tra le autorità giudiziarie degli Stati membri, proprio mediante il ravvicinamento delle relative legislazioni penali nel settore degli attacchi contro i sistemi di informazione. Com'è noto, la traiettoria di intervento inaugurata dalla Decisione Quadro è stata poi ulteriormente sviluppata con la Direttiva 2013/40/UE, la quale ugualmente si propone l'obiettivo di "ravvicinare il diritto penale degli Stati membri nel settore degli attacchi contro i sistemi di informazione", attraverso l'introduzione di norme di diritto sostanziale preordinate alla definizione delle fattispecie rilevanti e all'introduzione delle relative sanzioni: tutto ciò, nella prospettiva di "migliorare la cooperazione fra le autorità competenti"[15].

Com'è stato rilevato, se l'obiettivo primario del diritto penale transnazionale, al quale sono ascrivibili tutte le iniziative considerate, è quello di "promuovere la cooperazione interstatale", le disposizioni di diritto penale sostanziale non possono che risentire di questa "dipendenza" dalle norme procedurali, mancando di un solido sostrato valoriale condiviso[16].

In parallelo con le ultime fasi di tale evoluzione, a livello europeo si è tuttavia affermato un diverso modello d'intervento, che ha progressivamente affiancato (e poi quasi sostituito) le precedenti misure di repressione della criminalità informatica, segnando per certi versi la fine della centralità del diritto penale in questo ambito. Si fa riferimento, com'è noto, alla gestione "preventiva" della "sicurezza informatica", o cybersicurezza[17], che ha segnato il passaggio dal precedente approccio "difensivo"/"deterrente" – imperniato, per l'appunto, sul ricorso al diritto penale – a una diversa impostazione di stampo "protettivo"/"offensivo", fondata sulla previsione di obblighi di protezione delle infrastrutture cibernetiche da parte dei rispettivi titolari[18].

Esula beninteso dalla presente analisi una più diffusa ricostruzione del diritto extra-penale della cybersicurezza. Il tema merita un cenno, tuttavia, per due essenziali ragioni. Da un lato, perché esso segna (quanto meno nel contesto europeo) il passaggio a un modello "integrato", "proattivo e reattivo"[19] di difesa della sicurezza informatica: e ciò sul presupposto che per "ridurre drasticamente il *cybercrime*" sia necessario e più efficace, in luogo dello strumentario penalistico, lo sviluppo di risorse industriali e tecnologiche adeguate a garantire e rafforzare preventivamente la resistenza e la resilienza delle infrastrutture digitali[20]. Dall'altro lato, perché la stessa politica europea in materia di cybersicurezza ha attribuito a tale concetto una valenza polisemica – da mero requisito tecnico a vera e propria condizione di esistenza e di tutela dei diritti nel cyberspazio[21] –, che ha profondamente

14. Cfr. la Decisione Quadro 2005/222/GAI del Consiglio relativa agli attacchi contro i sistemi di informazione, del 24 febbraio 2005.
15. Cfr. la Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio. Con riferimento alle competenze penali dell'UE in materia di criminalità informatica, cfr. in generale Picotti 2011.
16. Cfr. Brunhober 2022, p. 244. Cfr. anche Sieber 1998, per il primigenio collegamento tra i due profili dell'armonizzazione (sostanziale) e della cooperazione (procedurale).
17. In argomento cfr. Flor 2019.
18. In questi termini cfr. Chesney 2020.
19. Cfr. Flor 2019, p. 456.
20. Cfr. la Comunicazione congiunta al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, JOIN(2013) 1, 7 febbraio 2013.
21. Cfr. De Vergottini 2019.

condizionato le stesse scelte statali in materia di tutela della sicurezza nazionale[22], con alcuni riflessi sulle opzioni politico-criminali *domestiche* e non più trans-nazionali.

Limitandoci ad alcuni cenni, già la prima "Strategia dell'Unione europea per la cybersicurezza: un ciberspazio aperto e sicuro" del 2013[23] rilevava l'esigenza di "sicurezza" del cyberspazio rispetto a "incidenti, attività dolose e abusi": da proteggere, dunque, tanto da "attacchi criminali, di natura politica o terroristica, o commissionati da uno Stato", quanto da "calamità naturali e errori non intenzionali". Le priorità strategiche affiancavano, tuttavia, alla riduzione del *cybercrime* mediante il diritto penale anche nuovi obiettivi di cyber-resilienza, cyber-difesa e cybersicurezza, da perseguirsi mediante interventi coordinati di carattere politico, economico e tecnologico, che consentissero "una protezione forte e una promozione efficace dei diritti dei cittadini" quale condizione della "sicurezza" del cyberspazio[24]. Ma il collegamento assiologico e funzionale tra cybersicurezza e "sicurezza" risulta ancora più esplicito nella successiva Comunicazione del luglio 2017, "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE"[25], nella misura in cui essa considera le "attività informatiche dolose" non più soltanto come minacce di consistenza "economica", eventualmente idonee a pregiudicare "il mercato unico digitale", ma anzitutto quali operazioni capaci di compromettere "il funzionamento stesso delle nostre democrazie, le nostre libertà e i nostri valori"[26].

In parallelo, a mutare sono anche i "soggetti" dai quali provengono le "cyber-minacce": non più solamente i "criminali motivati dal profitto", ma anche attori che agiscono per "motivazioni politiche e strategiche", la cui azione diventa tanto più allarmante alla luce del rilievo che "nella stragrande maggioranza dei casi, le possibilità di rintracciare i criminali sono minime e quelle di poter procedere ad azioni penali ancor più esigue"[27]. I pilastri strategici sono perciò individuati, tra gli altri, nel rafforzamento della resilienza agli attacchi, nella certificazione dei requisiti di cybersicurezza, nel potenziamento della risposta politica e di cyber-difesa. È significativo che l'obiettivo della creazione di una "deterrenza cibernetica efficace" non sia più perseguito mediante interventi sul piano del diritto penale sostanziale, ma soltanto attraverso la promozione di miglioramenti procedurali nell'identificazione degli autori degli attacchi e il miglioramento dell'effettiva "capacità di risposta" delle autorità di contrasto, anche attraverso la cooperazione investigativa e giudiziaria[28].

Analogamente, pure la coeva Risoluzione del Parlamento Europeo in materia di criminalità informatica[29], muovendo dal rilievo che il *cybercrime* non comporti soltanto pregiudizi economici, ma rappresenti attualmente una "minaccia" per "i diritti fondamentali delle persone fisiche" e "per lo Stato di diritto", articola la strategia di risposta tra prevenzione, responsabilizzazione dei fornitori di servizi e intensificazione della cooperazione di polizia e giudiziaria, anche con i Paesi terzi, nulla dicendo in materia di diritto penale sostanziale. Infine, anche nella successiva Strategia Europea per la Cybersicurezza del 2020[30], si rende ancor più esplicito che la "la cibersicurezza è parte integrante della sicurezza degli europei"[31] e che le minacce informatiche possono altresì pregiudicare

22. Cfr. Longo 2024, p. 203 ss.; Borriello–Fristachi 2022, p. 157 ss.
23. Cfr. ancora la *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*. Cfr. anche, in generale, Porcedda 2023, p. 45 ss.
24. Cfr. nuovamente la *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro.*
25. Cfr. la Comunicazione congiunta al Parlamento europeo e al Consiglio, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, JOIN(2017) 450, 13 settembre 2017; in argomento, cfr. Porcedda 2023, p. 49 ss.
26. Cfr. la Comunicazione *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE.*
27. *Ibidem*.
28. *Ibidem*.
29. Cfr. la Risoluzione del Parlamento europeo del 3 ottobre 2017, *Lotta alla criminalità informatica*, (2017/2068(INI)).
30. Cfr. la Comunicazione congiunta al Parlamento europeo e al Consiglio, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, JOIN(2020) 18, 16 dicembre 2020; cfr. ancora l'analisi di Porcedda 2023, p. 51 ss.
31. Cfr. ancora la Comunicazione *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*.

la salvaguardia dei diritti e delle libertà fondamentali dei cittadini. Anche in questo caso, il contrasto della cyber-criminalità si traduce in una serie di iniziative strategiche di resilienza e sovranità tecnologica, rispetto alle quali il contrasto della criminalità informatica è potenziato sul profilo della cooperazione, della diplomazia informatica e della cyberdifesa, in parallelo con la promozione di un cyberspazio "globale" e "aperto" che attribuisce anche agli Stati un obbligo di comportamento responsabile.

In altre parole, nella dimensione trans-nazionale ed europea, alla sempre maggiore consistenza valoriale del concetto di cybersicurezza corrisponde un progressivo arretramento della centralità del diritto penale sostanziale nella sua protezione, in parte in conseguenza dell'evidente mancanza di effettività di tale strumento, ma in parte anche per la crescente preponderanza della dimensione politica e strategica nella tutela delle infrastrutture digitali.

2. Prima traiettoria evolutiva: la riscoperta del diritto penale (globale) per la protezione della cybersicurezza

Ebbene, così sinteticamente ricostruita la "storia" recente del diritto del *cybercrime*, deve rilevarsi come – dopo oltre un decennio di tendenziale silenzio da parte dei legislatori, quantomeno nel contesto "regionale" europeo – negli ultimi anni si registri, invece, una "riscoperta" del diritto penale quale strumento di tutela del cyberspazio, persino su un duplice piano: da un lato, al livello propriamente *globale* e, dall'altro, nel contesto della legislazione penale *nazionale*. È proprio su tali tendenze che s'intende ora concentrare l'attenzione.

Muovendo dalla riscoperta del diritto penale al livello internazionale, i due principali strumenti che "ricollocano" nella dimensione globale la politica criminale di contrasto ai *cybercrime* sono la Convenzione delle Nazioni Unite contro il *cybercrime*, approvata nel 2024[32], e la *Draft Policy on Cyber-Enabled Crimes under the Rome Statute* dell'Ufficio del Procuratore della Corte Penale Internazionale, pubblicata nel 2025[33]. Si tratta, a ben vedere, di due strumenti coerenti con la visione espressa dall'Unione europea nella Strategia per la Cybersicurezza del 2020, relativa alla presa d'atto della dimensione "globale" del cyberspazio e, dunque, del necessario ruolo del diritto internazionale nella costruzione e nella tutela della cybersicurezza: tuttavia, entrambi tali strumenti, anziché focalizzarsi sul comportamento *degli Stati* nello spazio cibernetico, riguardano e definiscono la responsabilità *penale* individuale per la commissione di reati informatici.

Com'è noto, la Convenzione ONU contro il *cybercrime* è stata approvata dall'Assemblea Generale delle Nazioni Unite il 24 dicembre 2024 ed è stata poi denominata "Convenzione di Hanoi" a seguito della cerimonia ufficiale di apertura alla firma, avvenuta appunto ad Hanoi lo scorso 25 ottobre 2025. I lavori dell'*Ad Hoc Committee* incaricato della sua redazione sono durati oltre quattro anni e hanno richiesto una significativa opera di mediazione tra gli Stati, portatori di divergenti posizioni politico-criminali e di distinte "sensibilità" nel bilanciamento tra istanze di repressione della cyber-criminalità e garanzia dei diritti fondamentali[34]. All'esito di tale processo, l'approvazione del testo è stata salutata con favore dai primi commentatori, proprio in ragione della precedente "mancanza di uno strumento al tempo stesso universale e di portata generale nell'affrontare tutti gli aspetti dello specifico fenomeno criminale preso di mira"[35], nonché quale definitivo suggello del "processo di internazionalizzazione" nel contrasto alla criminalità cibernetica[36].

Benché il contenuto della Convenzione si sia infine assestato, nella parte del diritto penale

32. Cfr. United Nations, *United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*, 24 dicembre 2024.
33. Cfr. *Draft Policy on Cyber-Enabled Crimes under the Rome Statute*, pubblicata il 6 marzo 2025 dall'Ufficio del Procuratore presso la Corte Penale Internazionale.
34. Per un primo commento alla Convenzione cfr. Balsamo 2025.
35. *Ivi*, p. 244.
36. Cfr. in questi termini Mattarella 2025, p. 252.

sostanziale, su un elenco di fattispecie in buona parte sovrapponibile con quello della Convenzione di Budapest, nondimeno si ritiene che la Convenzione di Hanoi si differenzi dalle precedenti iniziative, nella misura in cui essa risponde – quantomeno a livello "aspirazionale" – al perseguimento di un'ideale di sicurezza cibernetica *globale*, rispetto al quale l'armonizzazione della legislazione penale sostanziale riveste una funzione cruciale e autonoma[37], non più dipendente dalle sole esigenze di cooperazione. Di tale mutamento di prospettiva si ha evidenza, ad avviso di chi scrive, sin dal Preambolo della Convenzione, che si apre con il dichiarato intento di perseguire "una politica penale globale per la protezione della società dalla cyber-criminalità", da attuarsi sia mediante una definizione condivisa delle fattispecie di reato, sia mediante un rafforzamento dei poteri di cooperazione internazionale.

Anche la struttura e i contenuti della Convenzione parrebbero confermare tale impressione. A differenza della Convenzione del Consiglio d'Europa – che colloca la tutela dei diritti e delle libertà fondamentali all'art. 15 e, dunque, tra le disposizioni comuni al solo diritto *procedurale* – la Convenzione di Hanoi situa la protezione dei diritti fondamentali (art. 6) tra le disposizioni generali, preliminari non soltanto alle norme processuali, ma anche agli obblighi di criminalizzazione, dei quali i diritti umani vengono così a costituire fondamento e limite. Nella medesima direzione, anche la lista delle fattispecie presenta alcune innovazioni rispetto al catalogo dei reati contemplato dalla Convenzione di Budapest, espressive di un'originale impostazione politico-criminale: tra tutte, ad esempio, (i) l'esplicito riconoscimento della connotazione "di genere" del *cybercrime*, del quale la fattispecie di "Non-consensual dissemination of intimate images" (art. 16) costituisce rilevante quanto inedito precipitato, nel contesto internazionale; e (ii) la definizione di circostanze aggravanti, per i reati che abbiano ad oggetto "critical information infrastructures" (art. 21). Del resto, non meno rilevanti, nella medesima prospettiva, sono le successive disposizioni in materia di assistenza e protezione delle vittime (art. 34) e di definizione delle "misure preventive" finalizzate a "ridurre le *opportunità*, presenti e future" di commissione di *cybercrime* (art. 53), tra le quali rientrano: iniziative di *public awareness*, il coinvolgimento dei *service provider*, la protezione dei c.d. *ethical hacker*, la reintegrazione dei cyber-criminali, o ancora la prevenzione della violenza di genere nel contesto digitale e la protezione delle persone vulnerabili. Proprio tali previsioni, espressive di una "strategia ampia di contrasto a tale fenomeno criminale", sono state individuate dai primi commentatori come il "valore aggiunto" e il tratto distintivo della nuova Convenzione[38].

Nella medesima direzione pare collocarsi anche la *Draft Policy on Cyber-Enabled Crimes under the Rome Statute*, pubblicata il 6 marzo 2025 dall'Ufficio del Procuratore presso la Corte Penale Internazionale. Prescindendo da una specifica disamina del contenuto della *Draft Policy* e dalle soluzioni tecniche che tale documento propone rispetto ad alcune questioni interpretative cruciali nel diritto (penale) internazionale[39], ai fini della presente indagine interessa piuttosto sottolineare come, anche in questo contesto, la dimensione "globale" della reazione – e l'affermazione dell'"impegno dell'Ufficio a condurre indagini rigorose e perseguire i reati *cyber-enabled*" – corrisponda proprio a una diversa considerazione della portata lesiva di tali reati. Invero, affermando che anche gli "unlawful and harmful uses of cyberspace"[40] possano rientrare nella giurisdizione della Corte dell'Aia, la *Draft Policy* implicitamente rileva come anche le violazioni informatiche possano attualmente rientrare tra quei *core crimes* che "minacci[ano] la pace, la sicurezza ed il benessere del mondo", come previsto dallo Statuto di Roma. In altre parole, coerentemente con il mandato della Corte, l'attenzione "internazionale" sui *cybercrime* dipenderebbe dalla relativa *gravità* e attitudine offensiva e non, invece, dalla dimensione transnazionale: invero,

37. Cfr. in questa prospettiva Wang 2025.
38. Cfr. in questi termini Balsamo 2025, p. 247 ss., nonché Mattarella 2025, p. 262, nel senso che la Convenzione introdurrebbe, in questo modo, "un diritto penale vittimologicamente orientato, sagomato anche sulle esigenze dei soggetti a vario titolo colpiti dal reato".
39. Cfr. in argomento l'analisi di Ambos 2015.
40. Cfr. la *Draft Policy*, cit., p. 4.

è anzitutto la natura *globale* e *vitale* dell'interesse protetto ad attrarre anche gli attacchi informatici entro l'ambito applicativo del "diritto punitivo della Comunità internazionale", in quanto potenzialmente costituenti "crimini contro la pace e la sicurezza del genere umano"[41].

3. Seconda traiettoria evolutiva: *pur un linguaggio nel mondo non (più) s'usa*. L'emergere dei legislatori penali nazionali nel cyberspazio

Come si anticipava, nella citata "riscoperta" del diritto penale quale strumento di contrasto alla criminalità cibernetica è possibile individuare anche una seconda traiettoria evolutiva. Si allude, in particolare, alla recente tendenza di alcuni legislatori nazionali a ricorrere sempre più spesso e in modo unilaterale al diritto penale per la protezione del cyberspazio (statale) rispetto a "minacce ibride"[42], talvolta – come si vedrà – pure attribuendo una proiezione applicativa extraterritoriale al diritto nazionale. Con il risultato che, se sino ad ora – come si è visto – la criminalità informatica ha rappresentato àmbito d'elezione del paradigma dell'armonizzazione penale, ora l'interprete è invece chiamato a riorientarsi in una "Babele" della tutela penale della sicurezza cibernetica.

Il punto di partenza di tale evoluzione – si ritiene – è il medesimo che è stato posto a fondamento della strategia europea per la cybersicurezza, nelle sue diverse fasi: la presa d'atto che, nel momento presente, la cyber-criminalità non costituisca più soltanto una minaccia per interessi economici individuali, ma possa minare la stabilità della società nel suo complesso, pregiudicare il funzionamento delle istituzioni e la tutela dei diritti dei cittadini, sì che la cybersicurezza diviene componente essenziale di quel concetto di "sicurezza" che storicamente rappresenta – non senza criticità – *cornice* e *fine* dello stesso intervento penale nazionale.

Muovendo da tale premessa, e riservando al prosieguo alcune considerazioni critiche, basterà per ora rilevare come, in prospettiva comparata, attualmente si moltiplichino le iniziative di criminalizzazione di "cyber-attacchi" o c.d. "minacce ibride", specialmente in aree ritenute strategiche per la sicurezza e l'interesse nazionale. Senza alcuna pretesa di esaustività, si forniranno alcuni esempi di tale tendenza politico-criminale.

Un primo essenziale riferimento è, in questa prospettiva, il *National Security Act 2023* adottato nel Regno Unito, che innova le disposizioni penali relative alla protezione della sicurezza nazionale, introducendo specifiche fattispecie per i casi di *espionage, sabotage* e *foreign interference*, quando realizzati nel dominio informatico[43]. Rilevante è, ad esempio, la fattispecie di cui alla Sect. 12 (*Sabotage*), che sanziona con l'ergastolo le condotte di danneggiamento (anche di sistemi elettronici e informatici) pregiudizievoli per la sicurezza o l'interesse nazionale, quando realizzate per conto di un potere estero (*foreign power*). Del pari, anche le fattispecie di *Espionage (Part I)*, benché non contengano un riferimento espresso all'uso di strumenti digitali, sono state riformate al preciso scopo di reagire alla "complessità delle moderne relazioni internazionali in un mondo interconnesso" e alle nuove opportunità di attacco rese possibili dalle nuove tecnologie[44]. Com'è stato rilevato anche dai primi commentatori, si tratta di fattispecie mediante le quali s'intende rafforzare la protezione della sicurezza nazionale contro minacce che, in considerazione dell'attuale evoluzione tecnologica, generalmente si realizzano proprio (e soltanto) nel dominio cibernetico (c.d. *cyber-espionage*); i paradigmi d'incriminazione prescelti si contraddistinguono per il ricorso a elementi piuttosto indeterminati (tra tutti, l'interesse o la sicurezza nazionale), nonché per l'arretramento della soglia d'intervento penale, derivante dal riferimento anche ad atti preparatori[45]. Al riguardo, è peraltro significativo sottolineare che, per espressa previsione, tali fattispecie si applicano *in ogni caso*, indipendentemente dalla nazionalità dell'agente e dal fatto che la condotta

41. Cfr. essenzialmente Vassalli 1999, p. 10.
42. Cfr. Sanz-Caballero 2023 e Billing–Feldtmann 2024.
43. Per un primo commento cfr. Scott 2024.
44. Cfr. National Security Act 2023, *Explanatory Notes*, in www.legislation.gov.uk, p. 7.
45. Cfr. Kendall 2024 e Scott 2024.

abbia avuto luogo nel territorio dello Stato, con una dichiarata proiezione extra-territoriale.

Un intervento del tutto analogo è riscontrabile anche in Polonia. Con legge del 17 agosto 2023[46], infatti, è stata approvata una modifica delle disposizioni penali relative al reato di *espionage*, allo scopo di adattarle al "costante mutamento della situazione geopolitica, al progresso tecnologico e al continuo cambiamento delle modalità operative dei potenziali autori"[47]: in particolare, la fattispecie è stata modificata per riformulare la stessa definizione dei comportamenti costituenti "spionaggio" (art. 130 del Codice penale polacco), nonché per criminalizzare espressamente la diffusione di disinformazione, e introdurre un significativo inasprimento delle pene. Allo stesso modo, anche nei Paesi Bassi è stata introdotta nel 2025 una riforma del Codice penale per criminalizzare nuove forme di spionaggio[48], tra le quali rientra anche il *digital espionage*, a tutela della sicurezza nazionale e delle infrastrutture critiche. Inoltre, il medesimo intervento normativo ha modificato diverse *computer-related offences*, per prevedere una circostanza aggravante per il caso in cui siano state realizzate per conto di un potere estero. Ancora, negli USA è stato di recente proposto il *Cyber Conspiracy Modernization Act*[49], che intende emendare il *Computer Fraud and Abuse Act* per criminalizzare espressamente, a livello federale, la c.d. *conspiracy* riferita ai *cybercrime*: con l'effetto, dunque, di creare un regime apposito e più severo per le condotte coordinate e organizzate, con un ulteriore arretramento della soglia dell'intervento penale (al livello dell'accordo-associazione), a tutela dell'ordine pubblico digitale[50].

Peraltro, lungo la medesima direttrice, non può non segnalarsi come in diversi Stati si registri altresì la progressiva attribuzione di poteri di intervento e contrasto della cyber-criminalità a organi appartenenti al comparto della sicurezza, della difesa e dell'*intelligence*, in luogo (o a completamento) delle tradizionali prerogative del magistero penale: è il caso, ad esempio, di un'imminente proposta che sarà a breve presentata in Germania[51], nonché di quanto già avvenuto in Giappone, dove, con la *Active Cyber Defense Law* del 2024, il concetto di cybersecurity è stato identificato con la "sicurezza nazionale e del popolo avverso attacchi informatici provenienti dall'esterno" ed è stato introdotto un modello di *active cyber defence* che coniuga misure tecniche e informative per la prevenzione e, soprattutto, la neutralizzazione dei cyber-attacchi[52].

Tratto comune a tutti gli interventi appena menzionati – per quanto possa osservarsi nei limiti dell'inevitabile cursorietà dell'indagine – è, in definitiva, il fatto che si tratti di iniziative "unilaterali" dei legislatori penali nazionali, i quali – quasi per la prima volta, nel dominio della criminalità cibernetica – non intervengono nel solco di indicazioni di armonizzazione a livello internazionale o europeo, ma elaborano autonome strategie politico-criminali, accomunate da alcuni stilemi che, utilizzando il lessico del diritto penale italiano, richiamano in vario modo la tutela della "personalità dello Stato", vale a dire degli interessi fondamentali della collettività, dalla sicurezza all'integrità nelle relazioni esterne. Del resto, già nella prospettiva del diritto costituzionale si è rilevato che l'attuale contenuto del concetto giuridico di cybersicurezza interessi tanto "complessivamente l'ordinamento statale", quanto "in dettaglio le sue componenti", dal momento che una qualsivoglia "aggressione tecnologica" è ora da ritenersi in grado di minacciare ad un tempo "la fruibilità dei diritti" da parte dei singoli soggetti appartenenti a un ordinamento, ma anche "gli interessi dello Stato"

46. Per un commento cfr. Burczaniuk 2024.
47. *Ivi*, p. 306.
48. Cfr. Government of Netherlands, *Legislation to be broadened to make more forms of espionage a criminal offence*, 18 marzo 2025.
49. Cfr. Congress of the United States of America, Cyber Conspiracy Modernization Act.
50. Cfr., in ordine al modello della *conspiracy*, Johnson 1973.
51. Cfr. Bundesministerium des Innern, *Strengthening cyber security – Federal Cabinet adopts key measures for increasing cyber security*, 27 agosto 2025.
52. Cfr. Mochinaga 2025.

nel suo complesso[53]. Di conseguenza, in parallelo con (e a prescindere da) il ruolo del diritto internazionale, è in definitiva con il diritto (penale) nazionale che gli Stati si trovano a reagire alle attuali minacce ibride, con un nuovo mosaico di incriminazioni che accomuna problematicamente regimi democratici e autoritari[54] e che non risulta più armonizzato a livello sovranazionale.

4. La recente trasformazione del diritto penale italiano: dal contrasto al *cybercrime* alla tutela della cybersicurezza nazionale

Un analogo riassestamento assiologico si registra, del resto, anche nel contesto nazionale. È ben noto, infatti, come storicamente il legislatore italiano sia intervenuto in maniera organica nell'ambito della criminalità informatica con la legge n. 547/1993[55] e con la successiva legge n. 48/2008[56], adeguando l'ordinamento alla prima Raccomandazione del Consiglio d'Europa e, successivamente, alla Convenzione di Budapest. È altrettanto noto, però, come, in occasione del primo di tali interventi, il legislatore abbia ritenuto che "la particolarità della materia non costituisse ragione sufficiente per la configurazione di uno specifico titolo"[57]. Si è deciso, quindi, di "ricondurre i nuovi reati alle figure già esistenti che ad essi, pur nella loro autonomia, appaiano più vicine", giacché "le figure da introdurre sono apparse subito soltanto quali nuove forme di aggressione, caratterizzate dal mezzo o dall'oggetto materiale, ai beni giuridici (patrimonio, fede pubblica, eccetera) già oggetto di tutela nelle diverse parti del corpo del codice"[58]. Secondo tale impostazione, dunque, le fattispecie riconducibili alla categoria della "criminalità informatica" sono state inserite nel codice penale in modo piuttosto disorganico e sono risultate, perciò, difficilmente riconducibili, nel loro complesso, a una strategia politico-criminale unitaria. A partire dal 2023, invece, si è registrato un deciso mutamento di prospettiva, che risulta del tutto coerente con quanto si è già evidenziato rispetto ad altre esperienze nazionali. Con il d.l. 105/2023[59], infatti, la materia della "criminalità informatica e cybersicurezza" è stata addirittura oggetto di un decreto-legge, a segnalarne l'urgenza politico-criminale. Ai fini che ora interessano, basterà sottolineare come tale intervento abbia collocato la criminalità informatica realizzata ai danni di sistemi pubblici nell'alveo delle fattispecie soggette ai poteri d'impulso e coordinamento del Procuratore Nazionale Antimafia e Antiterrorismo, al contempo autorizzando una serie di ulteriori strumenti investigativi, tra i quali le operazioni sotto copertura, nonché aprendo un canale informativo tra la "funzione" pubblica di cybersicurezza e le Procure.[60] Ancora più significativa è, nella medesima direzione, la legge 90/2024, che è intervenuta su più livelli a modificare le disposizioni penali relative alla cyber-criminalità[61]: per quanto ora più rileva, tale intervento ha determinato un'omogenea *specializzazione* delle fattispecie generali, introdotte anni addietro per recepire le indicazioni sovranazionali, al fine di costituire una reazione organicamente più severa rispetto alle condotte lesive della sicurezza

53. Cfr. De Vergottini 2019, p. 76.
54. Cfr. Sanz-Caballero 2023.
55. Rubricato "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".
56. Che costituisce ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica.
57. Relazione del Disegno di legge n. 2773, presentato dal Ministro di Grazia e Giustizia. – "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica" (XI Legislatura, divenuto legge 23 dicembre 1993, n. 547).
58. Cfr. ancora la Relazione del Disegno di legge n. 2773 e, in dottrina, Pecorella 2006.
59. Decreto-legge 10 agosto 2023, n. 105, "Disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché in materia di personale della magistratura e della pubblica amministrazione", convertito con modificazioni dalla legge 9 ottobre 2023, n. 137.
60. In generale, con riferimento a tale intersezione, cfr. Ricotta 2023.
61. Su questi temi cfr. Fiorinelli–Giannelli 2024 e i diversi contributi ivi raccolti.

informatica pubblica, al tempo stesso proiettando anche su tale forma di criminalità i paradigmi di contrasto tipici della lotta alla criminalità organizzata e al terrorismo, nel segno di una nuova emergenza politico-criminale[62]. Anche l'introduzione di una nuova fattispecie per la criminalizzazione dei c.d. attacchi *ransomware* (art. 629, co. 3, c.p.)[63] costituisce indice della progressiva "autonomizzazione" delle scelte di incriminazione in questa materia, a ulteriore riconferma dell'attuale priorità politico-criminale attribuita dagli Stati al contrasto delle minacce ibride, anche indipendentemente dagli strumenti di armonizzazione e cooperazione.

Il disallineamento rispetto ai paradigmi condivisi a livello transnazionale ed europeo risulta ancora più marcato in alcuni disegni di legge recentemente presentati in Parlamento, relativi alla (opportuna) definizione di una strategia nazionale per il contrasto agli attacchi *ransomware*. In estrema sintesi, le diverse proposte legislative (C.2366; S.1441; C.2318)[64], d'iniziativa di diverse forze politiche, convergono sulla ritenuta necessità di introdurre un sistema "integrato" per il contrasto e la gestione delle estorsioni informatiche, affiancando alla nuova fattispecie penale introdotta nel 2024 ulteriori misure extra-penali, tra le quali, ad esempio, un generale divieto di pagamento del riscatto per i soggetti inclusi nel c.d. Perimetro di Sicurezza Nazionale Cibernetica; l'istituzione di una task-force nazionale; la previsione di incentivi e di un fondo nazionale di supporto per le vittime di attacchi *ransomware*; la disciplina delle cyber-assicurazioni[65]. Prescindendo, anche in questo caso, da una più dettagliata disamina dei singoli disegni di legge, interessa soprattutto sottolineare il rilievo *diretto* che tali disposizioni proporrebbero di attribuire all'interesse e alla sicurezza nazionale nella concreta gestione e repressione degli attacchi, sul presupposto della "vulnerabilità del Paese" nel "panorama geopolitico" e della correlata necessità di "rafforzare la resilienza nazionale"[66]. Questa specifica impostazione emerge con chiarezza, infatti, dalla previsione – comune ai diversi d.d.l. – che il divieto di pagamento del riscatto sia derogabile con una "specifica determinazione del Presidente del Consiglio dei ministri" qualora l'attacco comporti "un rischio grave e imminente per la sicurezza nazionale", nonché dalla contigua previsione che proporrebbe di attribuire al vertice dell'Esecutivo altresì il potere di classificare un attacco *ransomware* come incidente che compromette la sicurezza nazionale, indipendentemente dal soggetto che l'ha realizzato, anche al fine della eventuale attivazione di misure di intelligence con finalità di contrasto in ambito cibernetico. Addirittura, in una direzione simile a quella rilevata in prospettiva comparata, si propone di prevedere che gli ufficiali di polizia giudiziaria delle forze dell'ordine possano svolgere le attività sotto copertura "anche su reti, sistemi informativi e servizi informatici utilizzati per compiere reati informatici posti al di fuori dei confini nazionali", con una proiezione extraterritoriale delle attività di contrasto. Nella convergenza tra diritto penale, discrezionalità politica e attività di intelligence si coglie la complessità dell'attuale "sistema di governo" della cybersicurezza nazionale, che si articola in un assetto "integrato e multilivello" di poteri pubblici, espressivi di un complesso equilibrio tra Stato-apparato e Stato-Nazione[67]. In prospettiva penalistica l'impatto appare duplice: da un lato, l'attrazione della cyber-criminalità all'area della criminalità *lato sensu* politica, in conseguenza della "politicizzazione" degli interessi protetti, come si dirà meglio nel paragrafo seguente; dall'altro lato, il moltiplicarsi di poteri (anche d'indagine) non

62. Sia consentito rinviare a Fiorinelli 2024.

63. In argomento, cfr. Corasaniti 2025.

64. Si fa riferimento ai disegni di legge: C. 2366 "Delega al Governo per la definizione di una strategia nazionale per il contrasto degli attacchi informatici a scopo di estorsione"; S. 1441 "Delega al Governo per la definizione di una strategia nazionale per il contrasto degli attacchi informatici a scopo di estorsione"; C. 2318 "Delega al Governo per la definizione di una strategia nazionale per il contrasto degli attacchi informatici a scopo di estorsione".

65. In generale, per una simile impostazione cfr. Teichmann 2025; Corasaniti 2025.

66. Cfr. il citato disegno di legge S. 1441.

67. Al riguardo, nonché in relazione ai rapporti tra sicurezza e cybersicurezza, è essenziale il rinvio a Macchia–Sferrazzo 2025; Giupponi 2024; Giupponi 2023; Carotti 2020; Lanzillo 2018.

soggetti alle garanzie penalistiche, ma rispondenti a valutazioni e opportunità politiche e strategiche. Ciò è particolarmente rilevante, ove si consideri come – a differenza di alcune esperienze comparate – nell'ordinamento italiano non si distingue il regime giuridico in base alla provenienza (estera o meno) dell'attacco. Un'impostazione ancor più marcatamente "difensiva" si rinviene, infine, negli ulteriori disegni di legge di recente presentazione (C.2607, C.2425, C.2417)[68] che propongono di introdurre una generale riforma della disciplina delle operazioni delle Forze Armate nello spazio cibernetico. Prendendo ad esempio il d.d.l. C. 2242, il "tema della difesa e della sicurezza dello Stato in ambito cibernetico" è individuato come area *trasversale*, nella quale gli attacchi alle infrastrutture critiche e quelli comunque "vitali" per gli interessi nazionali determinano la convergenza, in un'area pure coperta dalle rilevanti disposizioni penali, del codice dell'ordinamento militare, delle disposizioni in materia di Perimetro di Sicurezza Nazionale Cibernetica, dell'architettura nazionale di cybersicurezza, dell'intelligence in ambito cibernetico, nonché della Strategia nazionale di cybersicurezza. Il contenuto essenziale di tali proposte consiste nell'abilitare il comparto della difesa rispetto alle minacce cibernetiche relative alla sicurezza nazionale, in allineamento con l'intelligence, con l'attribuzione di un "ruolo preminente" allo "strumento militare" nello spazio cibernetico. Anche in tali disegni di legge emerge, dunque, il sempre più marcato collegamento della cybersicurezza con la "sicurezza nazionale" e i suoi "apparati", a tutela della stessa "sovranità" dello Stato, ora sviluppato secondo il diverso (ma non meno rilevante) paradigma della difesa militare.

5. Riflessioni conclusive: riconciliare *sicurezza* e *diritti* nella politica criminale "multilivello" del cyberspazio.

La disamina di tutti i più recenti interventi penalistici che si sovrappongono nell'ambito della criminalità informatica parrebbe suggerire come proprio il concetto di (cyber)sicurezza costituisca un efficace prisma interpretativo dell'attuale congerie di vettori giuridici, in quanto tale concetto aiuta a scomporre – ma al tempo stesso a connettere – le distinte traiettorie politico-criminali individuate in materia di *cybercrime*, nella tensione tra la ricerca di un equilibrio geopolitico globale e la tutela della sicurezza nazionale. A livello internazionale, infatti, il passaggio da un approccio regionale a un'impostazione globale riflette, come si è detto, l'emersione – almeno in senso aspirazionale – di un interesse realmente *comune* alla "pace e alla sicurezza nel cyberspazio"[69], perseguito per la prima volta mediante gli strumenti del vero e proprio diritto internazionale (penale). A livello nazionale, invece, come pure si anticipava, la connessione sempre più profonda tra il contrasto della criminalità informatica e la tutela penale della sicurezza nazionale è alla base della recente "riscoperta" del diritto penale, in parallelo con quel progressivo collegamento tra repressione criminale e cyber-difesa, che fa convergere nel settore della cybersicurezza uno spettro di poteri pubblici che si estendono dall'attività amministrativa, alla giurisdizione penale, fino al dominio militare. La categoria concettuale della sicurezza (riferita al dominio cibernetico) riconnette, dunque, le traiettorie di intervento che si affastellano *in subiecta materia*, dal momento che, tanto nella prospettiva internazionale, quanto a livello statale, la protezione (penale) dell'infrastruttura informatica e digitale è intesa quale strumento di

68. Si fa riferimento ai d.d.l.: C. 2607 "Modifiche al codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66, e altre disposizioni in materia di operazioni delle Forze armate in ambito cibernetico"; C. 2425 "Modifiche al codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66, e all'articolo 1 della legge 21 luglio 2016, n. 145, nonché introduzione dell'articolo 7-quater del decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, concernenti lo spazio cibernetico di interesse nazionale per la difesa e la sicurezza dello Stato e le operazioni delle Forze armate in ambito cibernetico"; C. 2417 "Modifiche al codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66, e altre disposizioni in materia di difesa dello spazio cibernetico e di operazioni delle Forze armate in ambito cibernetico".

69. Cfr. Wang 2025.

tutela della società nel suo complesso e della stessa sicurezza interna ed esterna degli Stati[70].

Ciò nondimeno, non può trascurarsi come i concetti di sicurezza internazionale e di sicurezza nazionale possano convergere sul piano teorico-ideale, ma nella prassi rischino di trovarsi spesso in una relazione di tensione o di potenziale conflitto: anzi, proprio le impostazioni più marcatamente "difensive" del cyberspazio registrate a livello statale, tanto più ove esse assumano anche un raggio d'azione extraterritoriale ovvero sviluppino pratiche di cyber-difesa attiva, rischiano di trasformarsi in fattori d'insicurezza, capaci di alterare l'equilibrio cibernetico globale. Ciò è a dire, in altre parole, che, nel più ampio quadro geopolitico, anche le recenti politiche penali si prestano a essere lette quali tracce di quel "protagonismo degli Stati" che contraddistingue l'attuale *race for the cyberspace*[71], con una potenziale tensione tra il livello nazionale e il livello internazionale.

D'altra parte, e soprattutto con riferimento agli ordinamenti statali, s'impone anche una diversa riflessione, a partire dalla centralità della cybersicurezza nelle recenti opzioni di politica criminale. Come si è visto, proprio entro tale cornice assiologica si colloca la reviviscenza di fattispecie di sapore "politico", che riportano alla luce l'esigenza di riconsiderare il "diritto penale del *cybercrime*" attraverso la lente dei diritti fondamentali, non più come *oggetto* di tutela, ma come *limite* alle scelte di incriminazione[72]. Proprio l'aggancio teleologico al concetto di "sicurezza nazionale", infatti, può far temere la tendenziale impermeabilità di tali iniziative politico-criminali – intese in senso ampio – al bilanciamento con altri diritti costituzionalmente garantiti, in tutta coerenza con il paradigma della legislazione penale dell'emergenza. In questa prospettiva, era stato già rilevato come la riflessione penalistica nel suo complesso non abbia ancora adeguatamente valutato in che misura la repressione penale della cyber-criminalità comprima – attraverso le stesse disposizioni *sostanziali* e non soltanto attraverso l'ampliamento dei poteri d'indagine – le libertà individuali: proprio in quanto materia di diritto penale "armonizzato", essa soffrirebbe al contempo il duplice limite di un debole ancoraggio in positivo a beni giuridici da tutelare, così come di un altrettanto debole ruolo dei diritti fondamentali quale limite alle scelte di incriminazione[73]. Se tale rilievo risulta senz'altro condivisibile, nel caso ora in esame la prospettiva che si apre pare ancora diversa: proprio l'ancoraggio *forte* al bene giuridico della "sicurezza nazionale" – variamente intesa al crocevia tra personalità interna e internazionale dello Stato, ordine pubblico, interesse pubblico – ha condotto diversi Stati a "rispolverare" fattispecie per lungo tempo inutilizzate (con lessico italiano: lo spionaggio, le "intelligenze con lo straniero", il disfattismo, i vari attentati all'integrità e all'indipendenza dello Stato, connessi o meno con un *foreign power*) e storicamente controverse, in quanto costruite attorno a beni giuridici di consistenza inafferrabile, come l'interesse politico o la sicurezza dello Stato, ritenuti dalla dottrina ben poco compatibili con i principi costituzionali in materia penale[74]. Non è questa la sede per una più compiuta disamina della categoria del "reato politico": sia consentito però rilevare come le più recenti riforme del *cybercrime* (anche e soprattutto nel panorama comparatistico) evochino proprio tale categoria concettuale e i ben noti, "radicali" problemi che essa solleva nell'ordinamento costituzionale[75]. Del resto, meritevole di un'eguale attenzione critica pare anche la parallela tendenza a fare della sicurezza non già oggetto ma, per così dire, "fine" e "modalità" della tutela, con l'erosione delle competenze dell'autorità giudiziaria, a favore di apparati d'ordine per definizione meno "garantiti",

70. Cfr. Brighi–Chiara 2021, pp. 19-20, e von Solms–van Niekerk 2013, p. 97 ss.

71. Cfr. Barozzi Reggiani 2025, p. 21, che riferisce alla *race for the cyberspace* non soltanto la componente "attivo-offensiva", ma anche quella "passivo-difensiva".

72. Cfr. Brunhober 2022, nonché in prospettiva più ampia Gohdes 2024.

73. Cfr. Brunhober 2022, p. 246.

74. Cfr. Insolera 1990, p. 457.

75. Cfr. in argomento l'analisi di Pulitanò 1989.

come quello di intelligence[76] o lo stesso comparto militare[77]. Anche a prescindere dall'arretramento delle garanzie che tale riassetto dei poteri potrebbe comportare, pare comunque essenziale evidenziare questa tendenza alla de-giurisdizionalizzazione del contrasto agli attacchi informatici, anche per la sua possibile collisione con la rinnovata architettura internazionale in materia di criminalità cibernetica, per le ragioni che già si anticipavano. In definitiva, emerge la necessità – di certo non nuova – di riconciliare *sicurezza* e *diritti*, nello sviluppo di una più organica politica criminale per il cyberspazio: ancor prima, però, è necessario aver ben chiaro quali (e quante) *sicurezze* e quali (e quanti) *diritti* ora convergano nello stesso concetto di cyberspazio e nella sua *governance* multilivello.

Riferimenti bibliografici

K. Ambos (2021), *International criminal responsibility in cyberspace*, in N. Tsagourias, R. Buchan (a cura di), "Research Handbook on International Law and Cyberspace", Edward Elgar Publishing, 2021

A. Balsamo (2025), *Spazio virtuale e processo penale: la nuova Convenzione ONU sul cybercrime*, in "Diritto penale e processo", 2025

G. Barozzi Reggiani (2025), *La* race for the cyberspace *degli Stati e il tema della cybersicurezza: tra sovranità e modelli di governance*, in "Rivista italiana di informatica e diritto", 2025, n. 2

F. Billing, B. Feldtmann (2024), *The Role of Criminal Law Approaches Against Hybrid Attacks*, in "Bergen Journal of Criminal Law and Criminal Justice", vol. 12, 2024, n. 2

G. Borriello, G. Fristachi (2022), *Stato (d'assedio) digitale e strategia italiana di cybersicurezza*, in "Rivista di Digital Politics", 2022

R. Brighi, P.G. Chiara (2021), *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE*, in "federalismi.it", 2021

D. Brodowski (2021), *The Emerging History of Transnational Criminal Law Relating to Cybercrime*, in N. Boister, S. Gless, F. Jeßberger (eds.),"Histories of Transnational Criminal Law", Oxford University Press, 2021

B. Brunhober (2022), *Criminal Law of Global Digitality. Characteristics and Critique of Cybercrime Law*, in M.C. Kettemann, A. Peukert, I. Spiecker (eds.), "The Law of Global Digitality", Routledge, 2022

P. Burczaniuk (2024), *The crime of espionage in new terms, i.e. in light of amendment to the Criminal Code of 17 August 2023*, in "Internal Security Review", vol. 30, 2024, n. 16

B. Carotti (2020), *Sicurezza cibernetica e Stato-nazione*, in "Giornale di diritto amministrativo", 2020, n. 5

R. Chesney (2020), *Cybersecurity Law, Policy, and Institutions (version 3.0)*, University of Texas Law, Public Law Research Paper No. 716, 2020

M. Chiavario, A. Perduca (2022), *Cooperazione giudiziaria internazionale in materia penale*, Giappichelli, 2022

J. Clough (2014), *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation*, in "Monash University Law Review", vol. 40, 2014, n. 3

G. Corasaniti (2025), *Strategie di contrasto al* ransomware *e nuove frontiere della criminalità informatica*, in "Il diritto dell'informazione e dell'informatica", 2025, n. 1

76. Cfr., al riguardo, essenzialmente Salvi 2023.

77. Cfr. in proposito, per una disamina dei poteri connessi alla "funzione di cybersicurezza", Macchia–Sferrazzo 2025, p. 123 ss.; Forgione 2022.

G. de Vergottini (2019), *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, in "Rivista AIC", 2019

G. Fiorinelli (2024), *La violenza mediata dalla tecnologia. Dogmatica, profili politico-criminali e interpretazione della nozione di violenza nel diritto penale delle tecnologie digitali*, Giappichelli, 2024

G. Fiorinelli, M. Giannelli (a cura di) (2024), *Il DDL Cybersicurezza (AC 1717). Problemi e prospettive in vista del recepimento della NIS 2*, in "Rivista italiana di informatica e diritto", sezione monografica, 2024, n. 1

R. Flor (2023), *Cyber-criminality: le fonti internazionali ed europee*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (diretto da), "Trattato di diritto penale – *Cybercrime*", Giappichelli, 2023

R. Flor (2019), *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, in "Diritto di internet", 2019

I. Forgione (2022), *Il ruolo strategico dell'agenzia nazionale per la cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna*, in "Diritto amministrativo", 2022, n. 4

A.R. Gohdes (2024), *Repression in the Digital Age. Surveillance, Censorship, and the Dynamics of State Violence*, Oxford University Press, 2024

T.F. Giupponi (2024), *Il governo nazionale della cybersicurezza*, in "Quaderni costituzionali", 2024, n. 2

T.F. Giupponi (2023), *Sicurezza e potere*, in "Enciclopedia del Diritto. I tematici V", Giuffrè, 2023

G. Insolera (1990), voce *Spionaggio*, in "Enciclopedia del diritto", vol. XLIII, Giuffrè, 1990

P.E. Johnson (1973), *The Unnecessary Crime of Conspiracy*, in "California Law Review", vol. 61, 1973, n. 5

S. Kendall (2024), *Espionage law in the UK and Australia: balancing effectiveness and appropriateness*, in "The Cambridge Law Journal", vol. 83, 2024, n. 1

M.L. Lanzillo (2018), *Lo stato della sicurezza. Costituzione e trasformazione di un concetto politico*, in "Ragion pratica", 2018, n. 1

E. Longo (2024), *La disciplina della cybersecurity nell'Unione europea e in Italia*, in F. Pizzetti, M. Orofino, A. Iannuzzi, S. Calzolaio, E. Longo (a cura di), "La regolazione europea della società digitale", Giappichelli, 2024

M. Macchia, G. Sferrazzo (2025), *Sicurezza e rischio tecnologico. La funzione di* cybersecurity, in "Diritto amministrativo", 2025, n. 1

A. Mattarella (2025), *Diritto penale e nuove tecnologie: dalla Convenzione Onu contro i reati informatici alle sfide dell'intelligenza artificiale*, in "Diritto penale e processo", 2025

D. Mochinaga (2025), *Rising sun in the cyber domain: Japan's strategic shift toward active cyber defense*, in "The Pacific Review", vol. 38, 2025, n. 2

C. Pecorella (2006), *Il diritto penale dell'informatica*, Cedam, 2006

L. Picotti (2011), *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in "Rivista trimestrale di diritto penale dell'economia", 2011

M.G. Porcedda (2023), *Cybersecurity, Privacy and Data Protection in EU Law. A Law, Policy and Technology Analysis,* Oxford University Press, 2023

D. Pulitanò (1989), voce *Delitto politico*, in "Digesto pen.", III, Utet, 1989

F.N. Ricotta (2023), *Agenzia per la cybersicurezza nazionale, sicurezza della Repubblica e investigazioni dell'Autorità giudiziaria*, in "Rivista trimestrale di diritto penale contemporaneo", 2023

G. Salvi (2023), *Intelligence e potere*, in "Enciclopedia del Diritto. I tematici, V", Giuffrè, 2023

S. Sanz-Caballero (2023), *The concepts and laws applicable to hybrid threats, with a special focus on Europe*, in "Humanities and Social Sciences Communications", 2023

S. Schjolberg (2008), *The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva*, in "Cybercrime Law", 2008

P.F. Scott (2024), *'State threats', security, and democracy: the National Security Act 2023*, in "Legal Studies", vol. 44, 2024, n. 2

U. Sieber (1998), *Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME Study*, 1998

F. Spiezia (2023), *Minaccia cibernetica e nuovi paradigmi della cooperazione giudiziaria internazionale: Il ruolo di Eurojust*, in "Sistema penale", 2023

F. Teichmann (2025), *Ransomware extortion in Europe: legal responses and mitigation strategies*, in "International Cybersecurity Law Review", vol. 6, 2025, n. 3

G. Vassalli (1999), *Statuto di Roma: note sull'istituzione di una Corte penale internazionale*, in "Rivista di Studi Politici Internazionali", vol. 66, 1999, n. 1

R. von Solms, J. van Niekerk (2013), *From information security to cyber security*, in "Computers & Security", vol. 38, 2013

X. Wang (2025), *Global (re-)framing of cybercrime: An emerging common interest in flux of competing normative powers?*, in "Leiden Journal of International Law", vol. 38, 2025, n. 2

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0252 • articolo sottoposto a peer review • pubblicato in anteprima il 13 gen. 2026

Sara Lilli

I dati come nuova valuta del cybercrime: mercati criminali, attori e responsabilità penale nell'economia digitale illecita

(Analisi a partire dal report di EUROPOL, IOCTA, 2025)

Il presente contributo si propone di esaminare l'emersione del dato quale risorsa centrale dell'economia criminale digitale, ricostruendo – a partire dal report di Europol IOCTA 2025 (*Steal, Deal and Repeat: How Cybercriminals Trade and Exploit Your Data*) – le dinamiche che ne favoriscono sottrazione, circolazione e sfruttamento sistematico. Lo studio si articola lungo due direttrici:(i) l'analisi della dimensione economico-criminologica del dato, inteso come target, mezzo e merce all'interno dell'*underground data economy*; (ii) la ricostruzione della filiera illecita degli *stolen data* nelle sue fasi di estrazione, distribuzione e riutilizzo, con particolare attenzione alla specializzazione degli attori coinvolti e agli ambienti di scambio. L'analisi consente così di mettere in luce il ruolo autonomo che il dato acquisisce nei processi criminali nel cyberspazio, nonché le conseguenti ricadute sull'impianto e sull'efficacia della tutela penalistica, chiamata a confrontarsi con forme di aggressione ai beni digitali che eccedono gli schemi tradizionali.

Cybercrime – Dati – Mercati illeciti online – Europol – Attori malevoli

Data as the new currency of cybercrime: criminal markets, actors and criminal liability in the illicit digital economy

This contribution examines the emergence of data as a central resource within the digital criminal economy, reconstructing – on the basis of Europol's IOCTA 2025 report (*Steal, Deal and Repeat: How Cybercriminals Trade and Exploit Your Data*) – the dynamics that enable its systematic theft, circulation and exploitation. The study develops along two lines of inquiry: (i) an analysis of the economic and criminological dimension of data, understood as target, tool and commodity within the underground data economy; (ii) the reconstruction of the illicit supply chain of stolen data across its phases of extraction, distribution and reuse, with particular attention to the specialisation of the actors involved and to the environments in which exchanges take place. The analysis highlights the autonomous role that data acquires within criminal processes in cyberspace, as well as the resulting implications for the structure and effectiveness of criminal-law protection, which is increasingly required to address forms of aggression against digital assets that fall outside traditional doctrinal frameworks.

Cybercrime – Data – Illicit online markets – Europol – Malicious actors

L'Autrice è dottoranda del Programma di Interesse Nazionale in Cybersecurity, affiliata presso la Scuola Superiore Sant'Anna di Pisa e la Scuola IMT Alti Studi di Lucca

La ricerca si inserisce nell'ambito del Progetto PNRR "Partenariato Esteso" PE 7 SERICS Security and Rights in the Cyber Space/ Spoke 1: Progetto CybeRights Codice identificativo: M4C2 11.3 - PE0000014 - CUPJ53C22003110001

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement - Parte 1*, a cura di Gaetana Morgante e Gaia Fiorinelli

1. Introduzione

Nell'analizzare le dinamiche contemporanee del cybercrime[1], emerge con particolare evidenza il ruolo centrale assunto dai dati personali[2], divenuti – oramai – non soltanto oggetto di tutela[3], ma anche vero e proprio strumento e prodotto dell'economia criminale. L'ultimo rapporto di Europol (*Internet Organised Crime Threat Assessment, 2025*)[4] dedica un'analisi specifica ai crescenti *illicit data markets*[5], mettendo in luce come l'informazione costituisca ormai una risorsa strategica contesa fra attori leciti e illeciti. Il dato viene sottratto, scambiato e utilizzato nuovamente come merce – una *commodity*

1. Sul punto, Wall 2024.
2. Per la definizione di dato personale occorre fare riferimento all'art. 4, n. 1, del Regolamento (UE) 2016/679 (GDPR), che qualifica come tale "qualsiasi informazione riguardante una persona fisica identificata o identificabile ('interessato'); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale". Quanto alla normativa interna, il richiamo è all'art. 4, comma 1, lett. b) del d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali o codice privacy), che definisce il dato personale come "Qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".
3. La crescente pervasività delle tecnologie digitali e la conseguente espansione della sfera informazionale dell'individuo sono state da tempo identificate in dottrina quali fattori di accresciuta vulnerabilità dell'identità personale nello spazio digitale, in questa prospettiva, si veda, *ex multis*, Gambini 2013, secondo cui "nella società dell'informazione, la grande quantità di dati personali generati dall'odierno mondo elettronico, combinata con le nuove tecnologie a disposizione, che rendono sempre più sofisticati e meno facili da rilevare gli strumenti di raccolta e trattamento delle informazioni personali, aumentano in modo esponenziale i rischi di esposizione delle persone a forme illegittime di intrusione nella propria sfera privata e di spoglio della propria identità".
4. Cfr. Europol 2025.
5. Cfr. Garkava–Moneva–Leukfeldt 2024.

– capace di generare valore economico, divenendo così una valuta funzionale al finanziamento e alla perpetuazione, nonché proliferazione, di attività criminali di natura transnazionale. La pervasiva digitalizzazione delle attività quotidiane e la progressiva interoperabilità dei sistemi informativi, tanto pubblici quanto privati, hanno determinato un ampliamento esponenziale della massa di informazioni suscettibili di esposizione a condotte criminose. In tale contesto, i dati personali, finanziari e tecnici – dalle credenziali di autenticazione alle informazioni di pagamento, sino agli elementi funzionali al governo di infrastrutture critiche – sono oggi al centro di un ecosistema illecito complesso, in cui differenti soggetti cooperano secondo logiche di specializzazione e interdipendenza.

Come rileva Europol, la possibilità di aggregare informazioni eterogenee e di sottoporle a processi di rielaborazione tramite sistemi di intelligenza artificiale generativa ha accresciuto in misura esponenziale la capacità trasformativa del dato sottratto, conferendogli una duttilità funzionale che ne moltiplica gli impieghi e ne amplifica la pericolosità. È su questo terreno, mobile e sfuggente, che si misura oggi una delle sfide più delicate per il diritto penale e per l'ordinamento dell'Unione europea: stabilire in che modo un'entità intangibile priva di consistenza fisica, ma dotata di un valore economico e strategico crescente, possa divenire simultaneamente oggetto di appropriazione[6], di circolazione e di condotte penalmente rilevanti.

In tale prospettiva, la riflessione sul dato si pone come passaggio necessario per indagare, nel prosieguo, circa la sua dimensione economica e criminologica, quella cioè che consente di coglierne la traiettoria – dal trattamento lecito allo sfruttamento illecito – all'interno di un sistema di mercato parallelo e che riproduce, *mutatis mutandis*, le logiche del cosiddetto *illicit data ecosystem*[7].

2. La dimensione economica e criminologica del dato

L'analisi di Europol mostra come il processo di sfruttamento del dato – sottratto – confluisca nella più ampia *underground economy*[8], vale a dire quell'area dell'economia digitale connotata da opacità strutturale e assenza di regolazione, nella quale si replicano logiche di mercato proprie dei contesti leciti. I circuiti che la compongono, difatti, si articolano secondo schemi tipici delle economie di piattaforma: divisione del lavoro, strutture reputazionali, meccanismi di *trust–building* e intermediazione tecnica[9]. Tali elementi contribuiscono a consolidare un ecosistema criminale strutturato, dove alcuni soggetti si occupano di ottenere l'accesso ai sistemi informatici compromessi (*initial access brokers*), altri di aggregare e organizzare le informazioni (*data aggregators* o *data brokers*), mentre ulteriori figure si dedicano alla rivendita o al riutilizzo dei dati in attività fraudolente (*end-user criminals*).

Sotto il profilo criminologico, la logica del profitto si innesta su un'infrastruttura tecnologica che consente al dato di assumere una natura riproducibile, potendo essere replicato infinite volte senza perdita di qualità e costi quasi nulli, non rivale, poiché l'uso di un dato da parte di uno non ne impedisce l'utilizzo anche da parte di altri, e cumulativa, in quanto il dato accresce di valore quando lo si

6. Non può essere taciuto, in questa sede, l'approdo cui è pervenuta la giurisprudenza di legittimità, nel ricondurre i dati informatici nell'alveo delle "cose mobili". In una pronuncia divenuta ormai riferimento imprescindibile, la Corte ha affermato che "i dati informatici, contenenti files, [sono] qualificabili 'cose mobili' ai sensi della legge penale e, pertanto, costituisce condotta di appropriazione indebita la *sottrazione* da un personal computer aziendale, affidato per motivi di lavoro, dei dati informatici ivi collocati, provvedendo successivamente alla cancellazione dei medesimi dati e alla restituzione del computer 'formattato'", secondo la ratio per cui "il file, pur non potendo essere materialmente percepito dal punto di vista sensoriale, possiede una dimensione fisica costituita dalla grandezza dei dati che lo compongono, come dimostrano l'esistenza di unità di misurazione della capacità di un file di contenere dati e la differente grandezza dei supporti fisici in cui i files possono essere conservati e elaborati"; v., in dottrina, Costabile 2005.
7. Sul punto, Howell–Fisher–Muniz et al. 2023; cfr. Europol 2025.
8. Cfr. Yip–Shadbolt–Tiropanis–Webber 2012; Greco–Greco 2020, nonché, in chiave ricostruttiva, Tanzi 1983.
9. Sul punto, Howell–Fisher–Muniz et al. 2023, pp. 298-300; Holt 2013.

combina con altri dati (si pensi ai dati anagrafici, i quali diventano più preziosi se associati a dati bancari o medici). L'informazione, privata del suo contesto originario, viene difatti reimpiegata in catene criminali complesse, ove la distinzione tra autore materiale, intermediario e beneficiario tende a sfumare. L'organizzazione delle condotte risponde a logiche imprenditoriali: il furto di dati (fase di *acquisition*) si collega alla rivendita (*distribution*), fino al reimpiego (*exploitation*), contribuendo ad alimentare un modello di *crime-as-a-service*[10] in cui l'informazione costituisce il prodotto principale. Ebbene, nei mercati *darknet* e nei forum specializzati, i dati vengono offerti secondo criteri di qualità, attualità e verificabilità[11], con un valore che varia in base alla tipologia – dati personali, finanziari, tecnici, aziendali – e al potenziale di impiego fraudolento. In tal senso, il dato opera quale vera e propria valuta criminale: è mezzo di pagamento, garanzia di credibilità e strumento di investimento all'interno di un'economia criminale che utilizza la criptovaluta come infrastruttura finanziaria primaria[12].

Il dato, in questo scenario, si configura simultaneamente come obiettivo, mezzo e merce: obiettivo degli attacchi, strumento per commettere ulteriori reati e merce di scambio in un'economia criminale digitalizzata.

2.1. Il dato come target

Alla luce dell'analisi svolta, il rapporto *IOCTA 2025*, individua proprio nella progressiva *datafication*[13] delle attività economiche e sociali la condizione abilitante che ha reso l'informazione digitale il *bersaglio privilegiato* di gruppi criminali organizzati operanti nello spazio cibernetico, e attivi tanto nei contesti finanziari quanto in quelli geopolitici.

Il dato diviene *target* poiché consente il conseguimento di ulteriori utilità criminali: il suo possesso permette di accedere a identità digitali, reti infrastrutturali, informazioni riservate e risorse economiche. Le intrusioni informatiche odierne non mirano soltanto al danneggiamento dei sistemi, ma alla esfiltrazione selettiva di informazioni suscettibili di sfruttamento o monetizzazione, innestandosi, *ab origine*, in un più ampio processo economico-criminale. Le campagne di *phishing*, i *data breaches* su larga scala, le violazioni di credenziali e i furti di identità costituiscono, ad oggi, le principali modalità di aggressione, spesso accompagnate da sofisticate tecniche di ingegneria sociale volte – anche – a indurre la vittima a fornire volontariamente dati personali. L'interesse criminale verso il dato quale *target* si articola lungo diverse categorie informative, tra loro accomunate dalla suscettibilità a generare valore illecito:

- *dati personali*, ossia informazioni idonee a identificare, anche indirettamente, un individuo (nome, indirizzo, credenziali di accesso, identificativi digitali), la cui appropriazione consente la duplicazione o l'usurpazione dell'identità, facilitando condotte di frode informatica, impersonificazione e abuso di identità;
- *dati finanziari*, quali numeri di carte di pagamento, credenziali bancarie o portafogli digitali, immediatamente monetizzabili nei circuiti dell'economia sommersa;

10. In proposito, il modello del *Cybercrime-as-a-Service* (CaaS) rappresenta una forma evoluta di criminalità informatica, fondata sulla vendita o noleggio di strumenti, competenze e infrastrutture digitali destinati alla realizzazione di reati nel cyberspazio. Il termine as-a-service trae origine da linguaggio informatico – ed economico – del *cloud computing* e si fonda sull'erogazione di risorse e competenze informatiche da parte di fornitori esterni, così permettendo a imprese e utenti di accedere a servizi digitali preconfigurati. Allo stesso modo, in ambito criminale, gli autori di reati possono acquistare o affittare servizi illeciti – come pacchetti di *malware*, accessi a sistemi compromessi o intere campagne di *phishing* – da fornitori specializzati che li mettono a disposizione su piattaforme dedicate. In tal modo, il *CaaS* trasforma l'attacco informatico in un vero e proprio mercato criminale strutturato, basato su logiche economiche di domanda e offerta, in cui la specializzazione dei fornitori e la riduzione delle competenze tecniche necessarie favoriscono la diffusione e la professionalizzazione delle attività illecite. Cfr. Akyazi–Van Eeten–Gañán 2021; Wall 2015; Europol 2023.
11. V. Howell–Fisher–Muniz et al. 2023, p. 302 ss.
12. V. Holt–Smirnova 2014.
13. Sul concetto di "*datafication*" v. Mejias–Couldry 2019.

– *dati tecnici o di sistema*, comprendenti codici di accesso, configurazioni di rete e credenziali amministrative, funzionali a movimenti laterali nei sistemi, escalation di privilegi o all'innesco di attacchi *ransomware*;
– *dati aziendali*, ossia insiemi informativi prodotti o detenuti da un'organizzazione nello svolgimento dell'attività economica, spesso dotati di rilevanza strategica o competitiva[14].

Secondo questa prospettiva, il dato quale *target* si configura come il punto di innesto di una catena criminosa che trascende la singola intrusione: l'informazione acquisita costituisce, simultaneamente, l'epilogo dell'aggressione e il presupposto funzionale di ulteriori fasi dell'iter delittuoso.

2.2. Il dato come mezzo

L'informazione sottratta non è mai statica: una volta fuoriuscita dal contesto originario, essa viene sottoposta a successive operazioni di (ri)utilizzo, arricchimento e rielaborazione, divenendo materia prima per finalità economiche, estorsive o strategiche. Le credenziali di accesso, i dati di pagamento e le informazioni aziendali, ad esempio, fungono da strumenti operativi idonei a condurre attacchi mirati (*targeted attacks*), a veicolare *malware* e a costruire campagne di disinformazione e manipolazione digitale. Il valore economico del dato si manifesta, inoltre, nella funzione abilitante rispetto ad altre forme di criminalità. Secondo Europol, i dati compromessi costituiscono la base operativa per attacchi *ransomware*, frodi finanziarie, attività di spionaggio industriale e sfruttamento sessuale minorile.

"Personal data is particularly valuable to the perpetrators […] as preparatory means of achieving their criminal goals"[15]: i dati personali costituiscono dunque mezzi preparatori, idonei a facilitare – e spesso a rendere possibile – la realizzazione dell'offesa principale. Si pensi alle frodi online, ad esempio, informazioni quali età, interessi, localizzazione, indirizzi e-mail, numeri di telefono, date di nascita o dati di pagamento consentono ai criminali di costruire profili accurati delle vittime, aumentando la verosimiglianza delle narrative fraudolente e facilitando l'accesso non autorizzato ai conti o alle risorse finanziarie dei soggetti colpiti; allo stesso modo, ovvero in ambito di *child sexual exploitation*, la disponibilità di informazioni personali consente l'individuazione, l'adescamento o la manipolazione di soggetti vulnerabili, accrescendo la portata offensiva dell'azione criminosa. Questa funzione *strumentale* permette ai dati di divenire mezzi di intermediazione tra più fasi del crimine: dalla compromissione iniziale dei sistemi, alla diffusione delle informazioni, fino al loro impiego per la realizzazione di ulteriori attività fraudolente o estorsive, nonché criminose.

2.3. Il dato come merce

Nella prospettiva delineata dal report *IOCTA 2025*, il dato sottratto non si esaurisce nella dimensione funzionale all'esecuzione dell'attacco, ma subisce un processo di conversione economica che lo trasforma in una vera e propria *merce* criminale. Europol osserva che l'informazione viene "stolen and converted into a commodity to be further exploited by other criminal actors in their operations", successivamente immessa in circuiti commerciali illeciti – *marketplaces* specializzati, forum sotterranei e canali cifrati *end-to-end* – ove assume una collocazione merceologica differenziata in ragione della tipologia, del grado di sensibilità e dell'utilità operativa per l'acquirente. Tale fenomeno, lungi dal rappresentare un mero riflesso accessorio dell'attacco informatico, si configura come elemento strutturale dell'economia criminale che opera nello spazio cibernetico. Gli ambienti digitali deputati allo scambio di informazioni illecitamente acquisite tendono, in maniera sempre più evidente, a organizzarsi secondo architetture che ricalcano, quasi specularmente, quei siti – legittimi – di *e-commerce* (si pensi, per esempio, ad Amazon), pur operando entro un perimetro contraddistinto da strutturale opacità e anonimato. L'esame dei principali forum internazionali evidenzia, in particolare, come la quota preponderante delle inserzioni – superiore, in taluni contesti, all'ottanta per cento del totale[16] – riguardi i dati necessari alla clonazione di carte di pagamento, le

14. Cfr. Lucas 2010; Eick–Fyock 1996.
15. Cfr. Europol 2025.
16. Giova rammentare un'analisi condotta nel 2014 sui principali forum criminali, dalla quale è emerso che l'84,3% dei beni offerti consisteva in dati sottratti – per lo più informazioni di pagamento e credenziali di accesso ad

credenziali di autenticazione, gli insiemi completi di dati identificativi e finanziari relativi agli utenti, nonché gli accessi a servizi bancari e commerciali. Tali beni vengono scambiati attraverso transazioni che si articolano secondo meccanismi consolidati di formazione del prezzo, sistemi reputazionali, procedure di verifica della qualità e una ripartizione funzionale dei ruoli tra gli attori coinvolti, delineando così un ambiente che presenta tratti di sorprendente stabilità interna nonostante la sua natura clandestina.

3. Lungo la filiera criminale degli *stolen data*

La ricostruzione empirica fornita dall'indagine di Europol consente di delineare la struttura operativa dell'economia criminale dei dati, organizzata secondo una sequenza funzionale di attività – estrazione, distribuzione e (ri)utilizzo (Fig. 1) – che ne delinea l'intera catena di trattamento illecito. Ciascuna fase è presidiata da attori specifici e si realizza attraverso mercati digitali interconnessi, nei quali il dato viene progressivamente trasformato da informazione a merce.

3.1. Estrazione

La fase di estrazione segna il momento genetico dell'intero ciclo criminale del dato, poiché in essa si realizza la prima (e più rilevante) violazione del potere di fatto e di diritto che il titolare esercita sull'informazione. È il frangente in cui l'illecito si manifesta nella sua dimensione sorgiva: l'acquisizione del dato – mediante intrusioni informatiche, tecniche di *exfiltration* o condotte di ingegneria sociale – segna il punto di rottura dell'originaria relazione tra il soggetto e la propria sfera informativa, traducendosi in una forma di spossessamento digitale. Gli attori che, ordinariamente, presidiano questa fase – noti come *initial access brokers* (*IABs*) – rappresentano il primo anello della catena criminale e operano con un grado di specializzazione tale da costituire un vero e proprio mercato primario dell'accesso illecito. Entro questo medesimo contesto operativo si collocano, *Advanced Persistent Threats* (*APT*) e gli *hybrid threat actors*, attori dotati di un livello di sofisticazione tecnica e di una capacità operativa tali da trascendere le finalità meramente lucrative proprie della criminalità informatica comune. Gli APT – spesso finanziati, sostenuti o direttamente organizzati da apparati statuali – perseguono obiettivi di lungo periodo, quali l'acquisizione indebita di informazioni di valore governativo, industriale o infrastrutturale, nonché attività di spionaggio digitale e compromissione sistemica di reti critiche. Gli *hybrid threat actors*[17], a loro volta, possono essere entità statuali o non statuali che impiegano una pluralità di strumenti – informatici e informativi – al fine di destabilizzare istituzioni, apparati pubblici o imprese strategiche, sfruttando l'ecosistema illecito del dato come moltiplicatore di capacità offensiva. I pacchetti di accesso[18], calibrati per livello di privilegio e tipologia di bersaglio, vengono poi venduti nei mercati digitali dedicati – forum specializzati, *darknet marketplaces*, canali cifrati – che ne consentono la circolazione secondo logiche di anonimato e di tracciabilità inversa.

3.2. Distribuzione

Una volta perfezionato l'accesso illecito e acquisita la disponibilità effettiva delle informazioni esfiltrate, il baricentro dell'azione criminosa si sposta fisiologicamente verso la fase della distribuzione. L'informazione viene immessa in circolazione all'interno di mercati digitali che riproducono, con fedeltà strutturale, le dinamiche e le architetture dei *marketplaces* legittimi. È in questa dimensione intermedia che il dato viene sottoposto a operazioni di selezione, aggregazione e correlazione, perdendo progressivamente ogni riferimento al suo contesto originario e assumendo una forma autonoma, standardizzata, commerciabile. Nei principali *darknet markets*, i *data brokers* operano

account digitali – commercializzati, poi, secondo schemi di determinazione del prezzo sensibili alle dinamiche concorrenziali interne alle piattaforme, Holt–Smirnova 2014.

17. Si veda, in merito, Maigre 2022.

18. In particolare, rientrano tra le offerte tipicamente commercializzate dagli *initial access brokers* le credenziali di accesso a servizi RDP, le credenziali VPN, gli accessi a firewall e dispositivi di rete, le credenziali per ambienti cloud, nonché backdoor già installate in sistemi aziendali e *footholds* persistenti, idonei a garantire una presenza continuativa dell'attaccante all'interno dell'infrastruttura compromessa, si veda Europol 2025.

come fornitori professionali di dataset, pubblicando annunci corredati da descrizioni tecniche, campioni di prova e sistemi reputazionali idonei a certificare l'affidabilità del venditore e la qualità del prodotto. Gli *administrators* e i *moderators*[19], dal canto loro, esercitano funzioni di gestione e controllo: amministrano le piattaforme, risolvono controversie, vigilano sul rispetto delle regole interne e garantiscono la correttezza delle transazioni, mediante l'impiego di sistemi *escrow*, fondati su criptovalute. Oltre ai tradizionali *marketplaces* del *dark web*, il panorama degli spazi di scambio conosce oggi l'emersione di canali paralleli, ospitati su piattaforme di messaggistica cifrata, come *Telegram* (in gruppi privati)[20], nonché altre piattaforme basate su crittografie *end-to-end* – che consentono transazioni rapide, decentralizzate e caratterizzate da un più elevato livello di anonimato, riducendo la vulnerabilità dei circuiti di scambio rispetto agli interventi di *take-down* delle autorità di *law enforcement*[21].

3.3. Riutilizzo

L'ultima fase della filiera è rappresentata dal riutilizzo – o *exploitation* – momento nel quale il dato illecitamente acquisito e successivamente distribuito viene reimpiegato quale *input* operativo per una pluralità di condotte ulteriori: campagne di *phishing* mirato, attacchi ransomware, frodi finanziarie multilivello, attività di spionaggio industriale, nonché forme di sfruttamento sessuale minorile. Gli attori che operano in questa fase sono gli *end-user criminals*, spesso inseriti in strutture transnazionali flessibili o in alleanze operative, la cui funzione primaria è la monetizzazione del dato e, più in particolare dataset, attraverso meccanismi estorsivi, appropriazioni fraudolente o successive rivendite a catena. È in tale segmento che il dato manifesta la sua massima forza criminogena: l'informazione sottratta genera nuova informazione utile al compimento di ulteriori reati, alimentando un ciclo potenzialmente infinito. Talvolta, il riutilizzo, per ciò stesso, non costituisce la mera conclusione del processo economico-criminale, ma il suo punto di rigenerazione: l'informazione reimpiegata produce infatti esiti ulteriori – nuove credenziali, nuovi accessi, nuovi elementi identificativi – i quali vengono, *ex novo*, immessi nella fase di distribuzione, secondo un modello che può qualificarsi, secondo le dovute cautele concettuali, come un'*economia circolare del dato illecito*. In questo senso, la fungibilità, la replicabilità e la non rivalità dell'informazione, come detto, costituiscono presupposti strutturali che ne consentono l'utilizzo reiterato e cumulativo.

4. Osservazioni conclusive

Senza concentrarsi sulle singole fattispecie penali che vengono in rilievo all'interno dell'ecosistema criminale del dato, come sopra descritto, il presente contributo ha inteso osservare l'approccio dell'ordinamento italiano a tale materia, evidenziandone gli elementi di continuità e, soprattutto, le criticità strutturali che emergono nell'attuale scenario tecnologico.

La legislazione penale italiana in materia di criminalità cibernetica si presenta, *ab origine*, come un insieme di norme incriminatrici eterogenee, frutto di interventi settoriali e frammentari (da ultimo con la legge 90 del 2024[22]), adottati non

19. Per una trattazione puntuale sulla struttura dei ruoli all'interno dei *darknet markets* si veda, *ex multis*, Peersman–Pencheva–Rashid 2021; White–Kakkar–Chou 2019.

20. Cfr. Garkava–Moneva–Leukfeldt 2024.

21. Un esempio significativo della capacità di coordinamento sovranazionale nel contrasto agli ecosistemi criminali digitali è costituito dall'operazione *Cookie Monster*. L'azione congiunta eseguita nell'aprile 2023 da FBI, Europol ed Eurojust, con il concorso di numerose autorità di *law enforcement* europee ed extra-UE, ha condotto allo smantellamento di *Genesis Market*, marketplace illecito di primaria rilevanza, specializzato nella commercializzazione di credenziali di accesso, cookie di sessione e *digital fingerprints* riconducibili a sistemi compromessi. L'operazione ha determinato il sequestro dell'intera infrastruttura telematica, nonché l'esecuzione di perquisizioni e arresti coordinati in oltre tredici Paesi, incidendo in modo decisivo su una piattaforma che metteva a disposizione milioni di identità digitali destinate a essere impiegate in attività fraudolente ed estorsive; v., nel sito di Europol, *Takedown of notorious hacker marketplace selling your identity to criminals.*

22. Circa le *disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*.

Fase	Attori principali	Mercati/ambienti di scambio
1. Estrazione	– Initial Access Brokers (IABs) – Hacker individuali o gruppi APT Insider Threats	– Forum specializzati deepweb e darkweb – Canali E2EE (Telegram, Discord) – Marketplace di accessi ("Access-as-a-Service")
2. Distribuzione	– Marketplace operators – Moderatori e venditori su dark web – Reti affiliate di broker	– Dark web markets (es. BreachForums, Hydra, RAMP) – Canali Telegram privati – Circuiti "trusted" peer–to–peer
3. Riutilizzo	– End-users criminali (frodi, ransomware, CSE) – Money mule networks – Gruppi di riciclaggio o disinformazione	– Piattaforme di pagamento illecite – Circuiti crypto off–chain – Network di frode integrata (ad es. BEC, phishing-as-a-service)

Tab. 1 — *Fasi, attori e mercati della filiera criminale del dato (tabella elaborata dall'Autrice sull'analisi condotta da Europol nel report IOCTA 2025)*

soltanto per colmare le lacune emerse nella prassi applicativa, ma anche per dare attuazione alle prescrizioni sovranazionali – in particolare agli stringenti obblighi di incriminazione derivanti dalla normativa europea e dagli atti del Consiglio d'Europa. Il primo atto organico fu la legge 23 dicembre 1993, n. 547, che introdusse nel Codice penale il primo nucleo sistematico di reati informatici, recependo (benché con ritardo rispetto ad ordinamenti tecnologicamente più avanzati) la lista minima e buona parte della lista facoltativa previste dalla Raccomandazione R(89)9 del Consiglio d'Europa. Con tale intervento, il legislatore si confrontò per la prima volta con condotte offensive aventi ad oggetto i nuovi "beni" dell'ecosistema digitale – dati, programmi e sistemi informatici – riconoscendo la necessità di una tutela penalistica differenziata. Tuttavia, l'ampiezza e la rapidità evolutiva dei fenomeni criminali che si sono progressivamente manifestati nel cyberspazio[23] hanno reso evidente l'impossibilità di racchiudere i crimini informatici entro un modello unitario e hanno orientato le scelte legislative verso una tecnica di *accostamento sistematico*. In assenza di un nuovo titolo dedicato esclusivamente ai "fatti di abuso della tecnologia informatica"[24] – soluzione espressamente scartata dal legislatore, che ritenne la peculiarità tecnologica insufficiente a giustificare una sezione autonoma del libro II[25] – le nuove incriminazioni sono state distribuite all'interno delle sezioni codicistiche esistenti "che ad essi, pur nella loro autonomia, sono apparse più vicine", prendendo atto che le diverse manifestazioni del fenomeno della criminalità informativa costituiscono "nuove forme di aggressione caratterizzate dal mezzo o dall'oggetto materiale, ai beni giuridici […] già oggetto di tutela nelle diverse parti del corpo del codice penale"[26]. La ricostruzione svolta consente di cogliere come l'evoluzione tecnologica – e, in particolare, la progressiva affermazione della dimensione cibernetica – abbia inciso in modo strutturale sul sistema penale, tanto sul versante delle categorie dogmatiche quanto su quello delle tecniche di tutela. L'odierno cyberspace, caratterizzato da automazione diffusa, iperconnettività globale e continua produzione di dati, non rappresenta più un mero contesto

23. Per un approfondimento, Picarella 2025.
24. Cfr. Pecorella 2000.
25. Nello specifico, si fa riferimento alla discussione in Parlamento di una proposta di legge in tema di criminalità informatica, d'iniziativa dei deputati Cicciomessere ed altri (Camera dei deputati, XI legislatura, n. 1174) che prevedeva, invece, l'introduzione di una nuova sezione nel Capo III del titolo XII del Codice penale, così nominata "Sezione IV - *Dei delitti in materia informatica e telematica*", v. sul punto Pecorella 2000.
26. Cfr. Camera dei deputati, XI legislatura, disegno di legge n. 2773. Presentazione del Ministro di Grazie e Giustizia (G. Conso), p. 3.

operativo delle condotte, ma un ambiente normativo e relazionale autonomo, nel quale si generano, circolano e si consumano nuove condotte penalmente rilevanti. In tale prospettiva, il diritto penale non può limitarsi a recepire passivamente nuove figure di reato, ma deve ripensare la propria funzione regolatoria alla luce delle trasformazioni che investono i concetti tradizionali di azione, evento, nesso causale e colpevolezza. Le condotte cibernetiche presentano, difatti, modalità esecutive non più interamente riconducibili alla diretta volontà dell'agente, non solo per effetto dell'automazione o dell'impiego di algoritmi adattivi, ma – nel caso specifico del mercato illecito dei dati – soprattutto per la spontanea dinamica di replicazione, diffusione e riutilizzo del dato sottratto, che tende a emanciparsi dal controllo dell'autore iniziale. Una volta immesso nel circuito criminale, il dato diviene oggetto di successive acquisizioni, manipolazioni e monetizzazioni ad opera di una pluralità indeterminata di soggetti, protraendo e ampliando l'offesa ben oltre il momento dell'intervento umano che ne ha provocato la prima compromissione. Ne emerge una frattura rispetto allo schema classico di imputazione penale, fondato su una relazione lineare tra agire, causalità ed evento, e ciò impone al penalista un profondo aggiornamento delle categorie concettuali e metodologiche tradizionali[27]. A ciò si aggiunge che molte condotte consumate nel cyberspace presentano caratteristiche ibride: esse si svolgono entro una dimensione materiale-immateriale nella quale l'offesa ai beni giuridici può manifestarsi in forme nuove – talvolta puramente funzionali o tecnologiche – ma non per questo meno gravi o meno meritevoli di tutela. La lesione della riservatezza informatica, la compromissione dell'integrità dei sistemi o la diffusione incontrollata di contenuti lesivi sono fenomeni che possono produrre effetti equivalenti, sul piano del danno, a quelli delle corrispondenti offese "tradizionali", quando non addirittura più penetranti e persistenti. Ne deriva la necessità di una lettura sistematica del concetto di bene giuridico protetto, all'interno della quale assumono un rilievo centrale beni nuovi o riqualificati, come la sicurezza delle reti, la riservatezza informatica e l'integrità del patrimonio digitale personale e collettivo. La loro tutela non è più esclusivamente rimessa all'autonomia del singolo, poiché la struttura stessa delle reti e l'interdipendenza globale dei servizi impongono l'introduzione di doveri di protezione, talvolta di natura pubblicistica, il cui inadempimento può integrare responsabilità penalmente rilevanti. Sul piano più strettamente sistematico, appare indispensabile delineare criteri di imputazione adeguati alla specificità dei fenomeni digitali. In particolare, assume rilievo la distinzione tra il momento di perfezione formale e quello di esaurimento sostanziale del reato, utile per comprendere le modalità di protrazione dell'offesa nel tempo digitale, nonché per definire la partecipazione di ulteriori soggetti – attivi od omissivi – che contribuiscono alla diffusione del fatto lesivo in rete. Tale distinzione risulta cruciale soprattutto nelle fattispecie commesse tramite sistemi automatizzati o tramite la circolazione virale dei contenuti on line. La stessa nozione di colpevolezza richiede un ripensamento critico: l'elemento psicologico deve essere valutato in relazione alla prevedibilità degli effetti tecnologici, alla scelta consapevole di impiegare sistemi autonomi, alla tolleranza del rischio inerente alla diffusione dei contenuti nel cyberspazio. Non si tratta di superare le garanzie del diritto penale liberale, ma di adattarne i criteri a condotte la cui effettiva portata lesiva si manifesta in un ambiente nel quale il controllo umano è solo parziale e spesso mediato da strumenti algoritmici. Affinché il diritto penale dell'informatica non si riduca a un un impianto ricostruttivo che opera per proiezioni, e non per realtà, è necessario ricordare che metafore e analogie possono svolgere un ruolo utile *soltanto ex post*, come strumenti descrittivi semplificatori, ma non possono – né devono – assolvere una funzione epistemica *ex ante*. È dunque imprescindibile che legislatore e interprete si confrontino direttamente con la struttura effettiva dei fenomeni digitali, evitando di lasciare che rappresentazioni metaforiche o semantiche – per quanto seduttive – orientino impropriamente la costruzione dogmatica. Solo emancipandosi da tali suggestioni sarà possibile restituire al concetto di "crimine informatico" una significatività sistematica, capace di ricomprendere anche le nuove forme di aggressione ai beni digitali, in particolare quelle che caratterizzano il

27. In questo senso, Picarella 2025.

mercato illecito dei dati e la loro circolazione criminale[28]. Ciò implica la necessità di un costante dialogo tra giuristi e tecnologi, affinché il diritto possa continuare a svolgere la sua funzione di garanzia, senza arretrare di fronte alle trasformazioni epocali della rivoluzione cibernetica, ma anzi governandole attraverso un apparato concettuale rinnovato e strumenti operativi adeguati alla complessità del mondo digitale.

Riferimenti bibliografici

S. Ahmed, M. Gentili, D. Sierra-Sosa, A.S. Elmaghraby (2022), *Multi-layer data integration technique for combining heterogeneous crime data*, in "Information Processing & Management", vol. 59, 2022, n. 3

A. Aktoudianakis (2020), *Fostering Europe's Strategic Autonomy – Digital sovereignty for growth, rules and cooperation*, in "European Policy Centre", 2020

U. Akyazi, M. van Eeten, C.H. Gañán (2021), *Measuring Cybercrime–as–a–Service (CaaS) Offerings in a Cybercrime Forum*, in "Proceedings of the Workshop on the Economics of Information Security (WEIS)" (Delft, 2021), Delft University of Technology, 2021

G. Costabile (2005), *Scena criminis, documento informatico e formazione della prova penale*, in "Diritto dell'informazione e dell'informatica", 2005, n. 3

S.G. Eick, D.E. Fyock (1996), *Visualizing Corporate Data*, in "AT&T Technical Journal", vol. 75, 1996, n. 1

Europol (2025), *Steal, Deal and Repeat: How Cybercriminals Trade and Exploit Your Data*, Internet Organised Crime Threat Assessment (IOCTA), Publications Office of the European Union, 2025

Europol (2023), *Cyber–attacks: The Apex of Crime-as-a-Service*, Europol Spotlight Report, Publications Office of the European Union, 2023

G. Fiorinelli (2023), *Nomina nuda tenemus? Lo statuto penalistico del crimine informatico tra mutamenti fenomenici e modificazioni semantiche*, in "Discrimen.it", 2023

M. Gambini (2013), *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in "Espaço Jurídico: Journal of Law", vol. 14, 2013, n. 1

T. Garkava, A. Moneva, E.R. Leukfeldt (2024), *Stolen Data Markets on Telegram: A Crime Script Analysis and Situational Crime Prevention Measures*, in "Trends in Organized Crime", 2024

F. Greco, G. Greco (2020), *Organised crime: underground economy and regulations to combat cybercrime*, in "European Journal of Political Science Studies", vol. 4, 2020, n. 1

T.J. Holt (2013), *Exploring the social organisation and structure of stolen data markets*, in "Global Crime", vol. 14, 2013, n. 2-3

T.J. Holt, O. Smirovna (2014), *Examining the structure, organization, and processes of the international market for stolen data*, in "Global Crime", 2014

C.J. Howell, T. Fisher, C.N. Muniz et al. (2023), *A Depiction and Classification of the Stolen Data Market Ecosystem and Comprising Darknet Markets: A Multidisciplinary Approach*, in "Journal of Contemporary Criminal Justice", vol. 39, 2023, n. 2

28. "D'altronde, l'esigenza di pervenire a una sistematizzazione del tema, in una prospettiva sostanziale, deriva non tanto da una astratta necessità di concepire il 'diritto penale del cybercrime' quale autonoma partizione sistematica, ma piuttosto dall'urgenza di far sì, ad esempio, che a tale fenomeno corrisponda un trattamento giuridico adeguato e omogeneo, e non, invece, come ora accade, conseguenze sanzionatorie del tutto disarticolate", così Fiorinelli 2023.

A. Lucas (2010), *Corporate Data Quality Management: From Theory to Practice*, in "Proceedings of the 5th Iberian Conference on Information Systems and Technologies" (Santiago de Compostela, 2010), 2010

M. Maigre (2022), *Cyber threat actors: how to build resilience to counter them*, in "Hybrid CoE Papers", 2022, n. 11

U.A. Mejias, N. Couldry (2019), *Datafication*, in "Internet Policy Review", vol. 8, 2019, n. 4

M. Pecorella (2006), *Diritto penale dell'informatica* (ristampa con aggiornamento), Cedam, 2006

L. Peersman, D. Pencheva, A. Rashid (2021), *Tokyo, Denver, Helsinki, Lisbon or the Professor? A Framework for Understanding Cybercriminal Roles in Darknet Markets*, in "Proceedings of the 2021 APWG Symposium on Electronic Crime Research (eCrime)", IEEE, 2021

L. Picarella (2025), *Criminalità in rete: dalle piattaforme illegali alle cybermafie*, Donzelli Editore, 2025

S. Tanzi (1983), *The underground economy. Causes and consequences of this worldwide phenomenon,* in "Finance and Development", vol. 20, 1983, n. 4

D.S. Wall (2024), *Cybercrime: The transformation of crime in the information age*, John Wiley & Sons, 2024

D.S. Wall (2021), *Cybercrime as a transnational organized criminal activity*, in F. Allum, S. Gilmour (eds.), "Routledge Handbook of Transnational Organized Crime", Routledge, 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

R. White, P.V. Kakkar, V. Chou (2019), *Prosecuting darknet marketplaces: challenges and approaches*, in "Department of Justice Journal of Federal Law & Practice", vol. 67, 2019

M. Yip, N. Shadbolt, T. Tiropanis, C. Webber (2012), *The digital underground economy: A social network approach to understanding cybercrime*, in "Digital Futures 2012: The Third Annual Digital Economy All Hands Conference", 2012

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0257 • articolo sottoposto a peer review • pubblicato in anteprima il 27 gen. 2026

Teresa Meccariello

Il cyberspazio tra impostazioni tradizionali e consolidamento normativo della "riservatezza"

Il lavoro analizza l'evoluzione dei reati informatici in Italia e il ruolo del dato e della riservatezza come beni giuridici autonomi. La ricerca empirica dell'Unità SERICS di Napoli evidenzia modalità operative ricorrenti e forte concentrazione territoriale dei procedimenti. La riservatezza è proposta come bene unitario di quarta generazione, distinguendo chiaramente tra accesso abusivo (615-*ter* c.p.) e frode informatica (640-*ter* c.p.), con prevalente negazione dell'assorbimento tra le due fattispecie. L'analisi sostiene l'esigenza di una protezione multilivello dell'informazione nella società digitale.

Riservatezza – Sistema informatico – Dato personale – Protezione – Sicurezza digitale

Cyberspace between traditional settings and the regulatory consolidation of privacy

The paper analyzes the evolution of computer crimes in Italy and the role of data and privacy as autonomous legal goods. Empirical research conducted by the SERICS Unit in Naples highlights recurring operational patterns and a strong territorial concentration of cases. Privacy is proposed as a unitary fourth-generation legal interest, clearly distinguishing between unauthorized access (Art. 615-ter c.p.) and computer fraud (Art. 640-ter c.p.), with the prevailing view rejecting the absorption between the two offenses. The analysis supports the need for multi-level protection of information in the digital society.

Privacy – Information system – Personal data – Protection – Digital security

L'Autrice è avvocato e assegnista di ricerca in cyber crime presso il Dipartimento di Scienze Politiche dell'Università degli Studi Federico II di Napoli

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement - Parte 1*, a cura di Gaetana Morgante e Gaia Fiorinelli

1. Cenni sulla evoluzione normativa e premessa metodologica

I reati informatici costituiscono una categoria delittuosa complessa, volta alla protezione di beni giuridici fondamentali quali la riservatezza, l'integrità e la disponibilità dei dati, la proprietà intellettuale nonché la sicurezza pubblica. La loro natura mutevole, intrinsecamente tecnica e spesso transnazionale ha reso la risposta normativa, sia a livello nazionale sia sovranazionale, talvolta frammentata e non sempre adeguata.

In Italia, l'evoluzione legislativa[1] è stata significativa: dall'introduzione della Legge n. 547/1993, al recepimento del Codice della Privacy (d.lgs. 196/2003)[2] e, più di recente, alle riforme in materia di cybersicurezza idonee a dare attuazione alle direttive europee NIS1 e NIS2, sino alla modernizzazione con la legge 90/2024 e con la normativa in tema di intelligenza artificiale. Nonostante tali interventi, la disciplina nazionale continua tuttavia a presentare elementi di disomogeneità: le fattispecie penali risultano spesso autonome e scollegate, e la normativa speciale – dalle disposizioni sul diritto d'autore alla disciplina di cui al d.lgs. 231/2000, fino al GDPR – si intreccia con il codice penale in modo non sempre sistematico.

La legge 547/1993 ha introdotto nel codice penale una serie di disposizioni destinate a formare il nucleo originario del diritto penale dell'informatica. Tra le principali, l'art. 615-*ter* c.p. (accesso abusivo a sistema informatico o telematico); l'art. 617-quater c.p. (intercettazione illecita di comunicazioni informatiche o telematiche); l'art. 635-bis e ss. c.p. (danneggiamento di dati e sistemi informatici); l'art. 640-*ter* c.p. (frode informatica). Si tratta di norme pionieristiche, che anticipano molte scelte poi recepite nella Convenzione di Budapest (2001)[3]. Tuttavia, tale intervento si

1. Per una più compiuta analisi delle fonti e dell'evoluzione legislativa in materia di reati informatici v. Flor 2019, p. 97-139.
2. Il Codice della privacy può essere considerato, in un certo qual senso, un duplicato della Carta di Nizza giacché la protezione dei dati personali assume al suo interno un ruolo di diritto con valenza del tutto autonoma. Infatti, con l'art. 1 del Codice è stata attribuita al diritto alla protezione dei dati personali una posizione distinta dal diritto alla riservatezza, venendo rimarcata la sua valenza di diritto fondamentale e la sua dimensione di libertà. Cfr. Costanzo 2008, pp. 49 e 58; Del Ninno 2006, pp. 3-5.
3. Flor 2019, p. 99 s.

concentrava prevalentemente sulla protezione dei sistemi e delle infrastrutture informatiche, lasciando in ombra la dimensione soggettiva dei diritti digitali e, in particolare, il valore del dato quale espressione dell'identità personale.

Il successivo Codice della Privacy (d.lgs. 196/2003), poi riformato alla luce del GDPR, ha segnato un cambio di paradigma: la protezione del dato personale è stata riconosciuta come manifestazione della dignità della persona (art. 2 Cost.) e della libertà personale (art. 13 Cost.). In dottrina questo passaggio è stato definito momento di "costituzionalizzazione del dato", ossia il riconoscimento dell'informazione come nuovo elemento di libertà individuale nella società digitale. Vale a dire "il paradigma tecnologico che si presenta come dominante, come fattore di liberazione della persona e di innovazione irresistibile, dunque, irrinunciabile"[4].

2. La ricerca dell'Unità SERICS Napoli: quadro metodologico e dati territoriali

L'attività di ricerca condotta dall'Unità SERICS di Napoli, nell'ambito dell'assegno finanziato dal progetto SERICS – PNRR MUR M4C2, ha comportato la raccolta e l'esame di un ampio numero di atti giudiziari provenienti dai Tribunali di Benevento, Avellino, Santa Maria Capua Vetere, Torre Annunziata, Napoli e Napoli Nord, con esclusione del solo Tribunale di Nola in ragione dell'insufficienza campionaria. Il lavoro si è concentrato sui reati informatici in senso proprio, vale a dire sulle fattispecie di cui agli artt. 615-*ter* e ss. c.p., analizzate nel periodo 2019-2024.

Sul piano dogmatico, la ricerca ha adottato la distinzione tradizionalmente accolta tra reati in cui il sistema informatico funge da mero strumento di offesa e reati in cui esso costituisce oggetto diretto dell'aggressione. L'indagine ha riguardato esclusivamente questi ultimi, in quanto maggiormente significativi ai fini della ricostruzione dell'evoluzione normativa e concettuale della materia. Tale scelta appare coerente con un processo di trasformazione che, a partire dalla legge 547/1993 sino alle riforme più recenti – tra cui la legge 90/2024 e la normativa sull'intelligenza artificiale – ha condotto a un progressivo ripensamento del bene giuridico sotteso ai delitti informatici e delle modalità di tipizzazione delle condotte[5]. L'evoluzione normativa, infatti, non si è limitata all'introduzione di nuove figure incriminatrici, come l'estorsione informatica, né all'inasprimento del trattamento sanzionatorio, ma ha investito il tema, più profondo, della configurabilità del dato come bene giuridico e della progressiva espansione della riservatezza entro lo spazio delle libertà costituzionalmente protette. In tal senso, si è sostenuto che "le importanti sentenze delle Corti Costituzionali tedesca, rumena e ceca, nonché quella della Corte di Giustizia, sembrano confermare la nascita di nuove forme di manifestazione dei diritti generali della personalità, che possono essere ricondotte al diritto all'autodeterminazione informativa ed al diritto alla riservatezza ed alla sicurezza dei dati e dei sistemi informatici. Il primo conferisce alla persona il potere di determinare, da un lato, il trattamento dei dati e delle informazioni ad essa attinenti, ampliando la tutela del diritto fondamentale alla libertà della vita privata e, dall'altro lato, il 'destino' delle 'aree informatiche' (cyberspace) in cui si manifesta la personalità umana. Il secondo, invece, garantisce l'interesse a non subire indebite interferenze nella sfera di rispetto e disponibilità di 'spazi informatici', indipendentemente dalla qualità (natura) o dalla quantità di dati e informazioni o dalla natura o dimensione dello spazio informatico di pertinenza del o dei soggetti 'titolari', nonché di tutelare l'integrità e la riservatezza dei dati e dei sistemi informatici assicurando così la correttezza e l'affidabilità dei rapporti giuridici che si instaurano nel cyberspace"[6]. Una parte rilevante di questa evoluzione, peraltro, si deve alla normativa speciale: si pensi alla legge sul diritto d'autore, al d.lgs. 231/2000, al Codice della privacy e al GDPR, che hanno anticipato e orientato quella progressiva "giuridicizzazione" del dato informatico oggi al centro del dibattito. In tal senso, si è posto al centro dell'attenzione il bene giuridico nel senso che, nel passaggio dall'on life

4. Caramaschi 2025, p. 40.
5. Sui crimini informatici, prendendo in considerazione la struttura delle fattispecie criminose ed i principali problemi che esse pongono, vedasi Amato Mangiameli–Saraceni 2019.
6. Flor 2010.

all'on line, si è cercato di capire quale fosse il bene giuridico oggetto di tutela nell'ambito del reato informatico[7].

C'è stato un iniziale ostracismo a utilizzare le categorie classiche dei diritti; diffidenza che col tempo è stata erosa grazie al lavorio della più autorevole dottrina e giurisprudenza. In tale senso, sono state pioniere le aperture in materia di domicilio informatico, che hanno equiparato lo spazio digitale al domicilio *tout court*. Del pari, pietra miliare è stato altresì il riconoscimento del dato informatico come *res* passibile di apprensione. Proprio la progressiva trasposizione delle libertà fondamentali dal reale al digitale, con progressiva ridefinizione anche di alcune fattispecie tipiche e con la parallela creazione di fattispecie *ad hoc* che, via via, il legislatore italiano ha introdotto nel frastagliato orizzonte della materia, ha consentito di riflettere sulla natura poliedrica e onnicomprensiva della riservatezza.

Il numero complessivo degli atti giudiziari acquisiti nei tribunali del distretto della Corte di Appello di Napoli è pari a circa 7.127, ripartite in percentuali che vedono Benevento detenere lo 0,25%, Santa Maria C.V. lo 0,81%, Avellino lo 0,94 %, Torre Annunziata il 5,61 %, Napoli Nord l'1,04% e Napoli il 91,37 %. Sulla base di tali indici valoriali è stato possibile ricavare una ripartizione percentuale che consente di misurare l'incidenza territoriale dei procedimenti relativi ai reati informatici in senso proprio. L'analisi proporzionale restituisce un quadro territoriale fortemente disomogeneo. Il Tribunale di Napoli, da solo, concentra oltre il 91% dei procedimenti esaminati, rivelando un'incidenza straordinariamente superiore rispetto agli altri territori del distretto. Tale dato, pur potendo riflettere la maggiore popolazione e il ruolo di polo metropolitano del distretto, suggerisce anche una più elevata capacità di emersione, segnalazione e trattazione dei reati informatici, nonché una maggiore densità di attività economiche e finanziarie appetibili per la criminalità digitale. Il valore rilevato per Torre Annunziata (5,61%) costituisce l'unico altro dato statisticamente significativo, confermando la presenza nel territorio vesuviano di un fenomeno criminale informatico strutturato e ricorrente. Gli altri tribunali presentano incidenze molto più basse (tutte inferiori all'1,1%), che possono derivare da diversi fattori: minore popolazione, minor radicamento dei reati informatici, minore capacità investigativa o diverso livello di digitalizzazione dei contesti socio-economici. Va inoltre sottolineato che la proporzione territoriale evidenzia come l'emersione statistica dei reati informatici sia significativamente influenzata sia dalla densità tecnologica sia dalla capacità delle forze dell'ordine e degli uffici giudiziari di intercettare e qualificare adeguatamente tali fenomeni. La fortissima concentrazione presso il Tribunale di Napoli potrebbe, quindi, riflettere non solo una maggiore frequenza dei reati, ma anche una maggiore sensibilità e strutturazione delle attività investigative in materia di cybercrime.

Dal punto di vista territoriale, i dati raccolti mostrano una significativa disomogeneità nell'emersione del fenomeno.

Sotto il profilo qualitativo emerge una notevole uniformità nelle condotte e nei modelli operativi. In tutti i tribunali esaminati i capi di imputazione risultano prevalentemente costruiti come concorso tra accesso abusivo e frode informatica, in perfetta coerenza con l'impostazione dogmatica che distingue la tutela del domicilio informatico dall'offesa al patrimonio conseguente all'alterazione o manipolazione dei dati. Nei tribunali maggiori si riscontrano, inoltre, anche contestazioni relative agli artt. 616, 617-*quater* e 617-*sexies* c.p., a dimostrazione di una gamma più ampia di condotte perseguite e di una maggiore sofisticazione dei casi esaminati. La figura dell'autore risulta generalmente riconducibile a un singolo individuo operante in concorso con soggetti in larga parte non identificati; nei casi in cui tali soggetti vengono individuati, essi risultano quasi sempre legati da rapporti familiari o fiduciari. Le dinamiche delle condotte, però, permettono di pensare a una criminalità informatica organizzata e strutturata sebbene non in maniera associativa. Le vittime, perlopiù inconsapevoli, comprendono privati cittadini, istituti bancari, società e Poste Italiane. Significativa è la quasi totale assenza delle pubbliche amministrazioni tra i soggetti passivi ovvero le persone offese, circostanza che indica una selezione delle vittime basata sulla vulnerabilità tecnica e sull'immediata disponibilità economica.

7. Picotti 2004, pp. 21-94.

La metodologia di esecuzione del reato è pressoché identica nei vari territori: essa si apre con un contatto fraudolento tramite posta elettronica o SMS (phishing), prosegue con l'induzione della vittima a comunicare dati sensibili o codici di accesso e culmina nell'intrusione nel sistema informatico e nella realizzazione dell'operazione fraudolenta. La costanza della tecnica, congiunta all'impossibilità di rilevare livelli elevati di competenza informatica negli autori, suggerisce l'utilizzo di strumenti fraudolenti facilmente reperibili e utilizzabili anche da soggetti privi di specifiche capacità tecnologiche.

Quanto alla qualificazione giuridica delle condotte, si rileva un quadro sostanzialmente coerente con gli orientamenti giurisprudenziali consolidati. Numerose decisioni, in particolare nell'area napoletana, qualificano l'accesso abusivo come antecedente non punibile quando esso costituisce mera condotta strumentale e priva di autonoma offensività rispetto alla frode informatica. Ciò si inserisce in un solco interpretativo secondo cui l'art. 615-*ter* tutela il domicilio informatico, mentre l'art. 640-ter si concentra sull'alterazione fraudolenta dei dati. Coerentemente, in alcuni casi il reato di frode informatica è stato ritenuto assorbente rispetto all'indebita utilizzazione dei codici di accesso prevista dall'art. 55, comma 9, d.lgs. 231/2007, quando tale condotta costituisce parte integrante del percorso criminogeno. Non mancano, tuttavia, pronunce che individuano forme di responsabilità concorrente anche in capo al titolare dell'account o dello strumento informatico sul quale confluiscono i fondi illeciti, come segnalato da una decisione del Tribunale di Benevento del 2022, ove è stata esclusa l'automatica irrilevanza della sua condotta rispetto alla frode.

3. La riservatezza come bene giuridico unico di quarta generazione

Proseguendo nell'analisi e alla luce dei risultati emersi dalla ricerca empirica condotta dall'Unità SERICS di Napoli, il tema della riservatezza come bene giuridico unitario di quarta generazione appare particolarmente fecondo e funzionale a ricomporre in un quadro sistematico coerente la frammentarietà normativa che caratterizza le fattispecie incriminatrici in materia di criminalità informatica. La progressiva emersione di comportamenti illeciti aventi ad oggetto dati, sistemi e processi informativi, nonché la sostanziale omogeneità rilevata nelle modalità operative delle condotte esaminate nel territorio distrettuale, confermano che l'oggetto della lesione penale non è più riconducibile alle categorie classiche del patrimonio o della libertà individuale, ma si concentra piuttosto sull'informazione come entità giuridica autonoma e come fulcro della dimensione digitale contemporanea. In questo senso, la nozione di riservatezza si presta a fungere da principio unificante[8], in grado di ricomprendere e sintetizzare la pluralità di interessi protetti dalle norme vigenti. Il bene giuridico della riservatezza assume così una configurazione estesa, che ricomprende non solo la protezione dei dati personali – intesa quale autodeterminazione informativa, coerente con il paradigma introdotto dal GDPR – ma anche la tutela dell'integrità, della disponibilità e della confidenzialità delle informazioni, indipendentemente dalla loro natura personale o meno. Tale ampliamento si giustifica alla luce della trasformazione digitale e dell'interconnessione permanente tra soggetti, sistemi e reti, nel quale la vulnerabilità informativa diviene direttamente incidente sulla sfera individuale e sulla dimensione collettiva. La tutela penale, pertanto, non può limitarsi a proteggere il singolo dato, ma deve necessariamente estendersi al contesto sistemico che ne consente la gestione, la conservazione e l'elaborazione, divenuto esso stesso oggetto di condotte criminose quali l'accesso abusivo, la manipolazione fraudolenta o l'illecita appropriazione.

La convergenza funzionale delle fattispecie previste dagli artt. 615-*ter* e ss. c.p. mostra chiaramente come il legislatore abbia tentato di costruire un sistema di protezione articolato ma tendenzialmente ispirato a un medesimo nucleo assiologico: la tutela dell'informazione in quanto tale[9]. Le sovrapposizioni rilevate nella prassi applicativa, e confermate dall'analisi delle sentenze del distretto di Corte di Appello di Napoli esaminate nel periodo 2019-2024, evidenziano come le violazioni dell'integrità o della disponibilità dei dati rappresentino spesso l'antecedente logico necessario per la successiva aggressione al patrimonio mediante

8. Troncone 2020.
9. Sul punto, per una più compiuta analisi, vedasi Galiano–Leogrande–Massari–Massaro 2020.

frode informatica, sicché i due piani risultano inevitabilmente intrecciati. L'idea di un bene giuridico unitario, lungi dall'essere una costruzione meramente teorica, trova dunque riscontro concreto nel fatto storico, nella ripetizione delle modalità esecutive e nella costante contiguità tra condotte che, pur astrattamente distinte, si realizzano nella medesima dimensione informativa.

Dottrina autorevole[10] ha da tempo posto in evidenza la natura poliedrica della riservatezza, intesa come bene giuridico complesso e capace di abbracciare interessi individuali, collettivi e, in alcune ipotesi, persino sovraindividuali. Le elaborazioni recenti hanno ulteriormente precisato tale prospettiva, sottolineando come la riservatezza si configuri non solo quale diritto alla protezione dei dati, ma anche quale garanzia dell'identità digitale e presupposto strutturale della fiducia nei sistemi informativi. In questa direzione, la riservatezza assume una natura sistemica, idonea a sostenere l'intero impianto sociale ed economico fondato sull'elaborazione digitale, e ciò spiega perché la sua lesione, anche quando apparentemente minima, possa generare effetti espansivi potenzialmente dirompenti.

Una simile prospettiva consente di superare la tradizionale frammentazione normativa e interpretativa, orientando l'intervento punitivo verso la protezione dell'informazione come elemento essenziale della persona e della collettività. Ciò offre una chiave di lettura coerente non solo dei reati informatici attualmente codificati, ma anche delle nuove sfide poste dall'evoluzione tecnologica[11]: dall'intelligenza artificiale all'Internet delle cose, dalla blockchain ai sistemi predittivi basati su grandi basi di dati. In tali contesti, l'informazione non è più un mero supporto, bensì la struttura stessa che sostiene l'interazione tra individui, enti e infrastrutture, divenendo così un bene giuridico di primaria rilevanza. L'adozione della riservatezza come bene giuridico unitario permette, quindi, di fornire una risposta penalistica più razionale, proporzionata e orientata alla sostanza del fatto lesivo, costituendo al contempo un criterio guida per il necessario aggiornamento della disciplina in un ecosistema tecnologico in rapida e continua evoluzione[12].

4. Riflessioni conclusive

Nel quadro interpretativo ricostruito alla luce della riservatezza come bene giuridico unitario, la questione dell'assorbimento tra il delitto di accesso abusivo a sistema informatico (art. 615-*ter* c.p.) e quello di frode informatica (art. 640-*ter* c.p.) pone un problema sistematico di particolare rilevanza, poiché consente di misurare la tenuta dell'assetto attuale della parte speciale rispetto all'evoluzione tecnologica. Benché nella pratica applicativa le due condotte si manifestino spesso in un *continuum* fattuale – come confermato dai dati raccolti nella ricerca SERICS, in cui l'accesso abusivo rappresenta frequentemente la fase prodromica della frode informatica – l'orientamento prevalente di dottrina e giurisprudenza nega, allo stato, la possibilità di un assorbimento sistematico. Ciò in quanto i due reati tutelano beni giuridici ontologicamente distinti: l'art. 615-*ter* c.p. protegge l'integrità, la riservatezza e la disponibilità del sistema informatico quale "domicilio digitale", mentre l'art. 640-*ter* c.p. ha per oggetto la tutela del patrimonio contro condotte fraudolente realizzate mediante manipolazione o inganno informatico.

La differenza strutturale tra i beni giuridici coinvolti è stata ribadita da un'ampia parte della dottrina e dalla giurisprudenza. Pur potendo le condotte concatenarsi nel fatto storico, l'accesso abusivo rappresenta una lesione autonoma e antecedente di un bene diverso da quello patrimoniale, sicché non può essere attratto nel paradigma del delitto complesso[13]. Ciò nella misura in cui ai fini dell'assorbimento, non basta la mera strumentalità dell'accesso alla frode; ciò che rileva è la coincidenza o meno dei beni giuridici protetti, essendo l'istituto del concorso apparente fondato su un criterio di specialità e non di mera consequenzialità

10. Troncone 2020.

11. Parodi–Sellaroli 2020, pp. 681-682.

12. Frosini 1981, p. 196. Per l'Autore L'ingresso nella società digitale ha dato vita ad un processo di astrazione dell'uomo dalla natura verso un mondo virtuale con la conseguenza che i problemi non possono essere ricondotti alle categorie tradizionali, ma occorre, invece, riconsiderare i valori e le forme di tutela.

13. Fiandaca–Musco 2021, pp. 431-434.

cronologica[14]. In questa prospettiva l'accesso abusivo determina una compromissione dell'integrità del sistema informativo che non può considerarsi assorbita da una successiva lesione patrimoniale, poiché si realizza su un piano logico e offensivo distinto, avente una sua piena rilevanza lesiva.

La giurisprudenza più recente si colloca sul medesimo solco interpretativo. La Corte di Cassazione ha infatti affermato che la condotta di accesso abusivo non può ritenersi assorbita nel delitto di frode informatica, trattandosi di fattispecie che "preservano beni giuridici non sovrapponibili: il domicilio informatico e il patrimonio" (Cass., sez. V, 27 giugno 2021, n. 28418). La Suprema Corte ha ulteriormente precisato che, anche quando l'accesso costituisce la condizione necessaria per la successiva frode, esso non si riduce a un mero momento preparatorio, ma conserva un'autonoma valenza offensiva, in quanto incide sulla sfera di riservatezza del titolare del sistema (Cass., sez. II, 9 marzo 2021, n. 9874). Tale orientamento risulta coerente con la ricostruzione dottrinale della riservatezza come bene giuridico autonomo e multidimensionale: la violazione dell'integrità del sistema non si esaurisce nella lesione patrimoniale, ma costituisce già di per sé un'aggressione alla "identità informatica" del soggetto, elemento essenziale della sua sfera personale nella società digitale.

Ne deriva che il concorso materiale tra art. 615-ter e 640-*ter* c.p. è, allo stato, la soluzione ordinaria, poiché l'azione lesiva si dispiega su piani distinti che il legislatore ha voluto presidiare autonomamente. La possibilità di assorbimento, evocata in talune pronunce isolate come ipotesi eccezionale, non trova fondamento nel principio di specialità né appare compatibile con il disegno complessivo di tutela delineato dalla parte speciale. L'accesso abusivo, infatti, non è una condotta meramente ancillare, ma un'aggressione diretta all'integrità del sistema informativo, che richiede una reazione penale distinta anche quando costituisce la premessa della frode.

L'impianto normativo vigente rivela così la volontà del legislatore di garantire una protezione multilivello dell'informazione: prima come forma di riservatezza, poi come risorsa economicamente rilevante. Pertanto, la separazione tra le due fattispecie – e la conseguente esclusione di un assorbimento sistematico – risulta pienamente coerente con la ricostruzione della riservatezza quale bene giuridico autonomo e centrale nel diritto penale informatico. Solo riconoscendo la duplice dimensione dell'offesa (al sistema e al patrimonio) il diritto penale può garantire una tutela adeguata alla complessità delle condotte criminose digitali, evitando soluzioni riduttive che finirebbero per impoverire la protezione dell'informazione quale infrastruttura essenziale della società contemporanea.

Pur nel quadro ricostruttivo che attribuisce ai reati informatici una tutela multilivello dell'informazione, non manca una parte minoritaria della dottrina che, muovendo da un approccio maggiormente pragmatico, ha ipotizzato la possibilità di configurare un rapporto di assorbimento tra il delitto di accesso abusivo (art. 615-*ter* c.p.) e il delitto di frode informatica (art. 640-*ter* c.p.) quando la condotta di intrusione nel sistema costituisca un mero segmento esecutivo della fraudolenta manipolazione informatica. Secondo questa lettura, l'accesso illecitamente realizzato sarebbe del tutto "assorbito" nella successiva alterazione del sistema quando non esprime un autonomo disvalore offensivo, ma rappresenta soltanto la fase strumentale necessaria alla lesione patrimoniale. Nelle ipotesi di fraudolenta sottrazione di credenziali bancarie tramite intrusioni minime, è stato affermato, per esempio, che può astrattamente delinearsi un rapporto di progressione criminosa tale da consentire un concorso apparente di norme, poiché "la condotta di penetrazione nel sistema si esaurisce nella realizzazione dell'inganno informatico"[15]. In termini simili, è stato osservato che qualora l'accesso abusivo abbia un livello di offensività "praticamente neutro", l'intera sequenza possa essere sussunta nella fattispecie di frode informatica, configurandosi una sorta di specialità funzionale "in senso inverso"[16]. Tale impostazione, tuttavia, rimane allo stato del tutto minoritaria e non recepita dalla giurisprudenza, la quale continua a ritenere che l'accesso abusivo leda autonomamente la sfera di riservatezza informatica, mentre la frode informatica aggredisce il

14. Mantovani 2021, pp. 406-409.

15. Palazzo 2018, pp. 512-514.

16. Picotti 2019, pp. 243-245.

patrimonio, impedendo ogni configurazione di assorbimento strutturale. La ricostruzione tradizionale – oggi dominante – valorizza la pluralità dei beni giuridici coinvolti[17] e la necessità di mantenere distinti i due titoli di reato, anche quando l'intrusione costituisce il presupposto logico della manipolazione fraudolenta. Tuttavia, la stessa esistenza di una dottrina che paventa l'assorbimento dimostra come il tema resti aperto e come la crescente unitarietà del bene della riservatezza, inteso in senso esteso, continui a stimolare una riflessione sistematica sulla possibilità di riordinare le fattispecie informatiche alla luce di una maggiore coerenza offensiva.

Riferimenti bibliografici

A.C. Amato Mangiameli, G. Saraceni (2019), *I reati informatici. Elementi di teoria generale e principali figure criminose*, Giappichelli (II ed.), 2019

O. Caramaschi (2025), *Il costituzionalismo al cospetto dell'intelligenza artificiale: nuove sfide, quali soluzioni?*, in "Rivista italiana di informatica e diritto", 2025, n. 1

P. Costanzo (2008), *La dimensione costituzionale della privacy,* in G.F. Ferrari (a cura di) "La legge sulla privacy dieci anni dopo", EGEA, 2008

A. Del Ninno (2006), *La tutela dei dati personali. Guida pratica al Codice della privacy (d.lgs. 30.6.2003, n. 196)*, Cedam, 2006

G. Fiandaca, E. Musco (2021), *Diritto penale. Parte speciale*, vol. II, Zanichelli, 2021

R. Flor (2019), *Cyber-criminality: le fonti internazionali ed europee*, in "Cybercrime – Diritto e procedura penale dell'informatica", Utet, 2019

R. Flor (2010), *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet*, in "Diritto Penale Contemporaneo", 2010

V. Frosini (1981), *Il diritto nella società tecnologica*, Giuffrè, 1981

A. Galiano, A. Leogrande, S.F. Massari, A. Massaro (2020), *I dati non personali: la natura e il valore*, in "Rivista italiana di informatica e diritto", 2020, n. 1

F. Mantovani (2021), *Diritto penale. Parte speciale*, Cedam, 2021

F. Palazzo (2018), *Corso di diritto penale. Parte speciale*, Giappichelli, 2018

C. Parodi, V. Sellaroli (2020), *Diritto penale dell'informatica. Reati della rete e sulla rete*, Giuffrè, 2020

L. Picotti (2019), *Diritto penale e tecnologie informatiche: una visione d'insieme*, in "Cybercrime", Utet, 2019

L. Picotti (2004), *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in "Il diritto penale dell'informatica nell'epoca di Internet", Cedam, 2004

P. Troncone (2020), *La tutela penale della riservatezza e dei dati personali: profili dommatici e nuovi approdi normativi*, Edizioni Scientifiche Italiane, 2020

17. Parodi–Sellaroli 2020, pp. 712-723.

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0245 • articolo sottoposto a peer review • pubblicato in anteprima il 11 nov. 2025

Pasquale Troncone

Il progetto di un assetto normativo autonomo per la sicurezza dei sistemi informatici e dei dati

La complessità normativa che sta investendo negli ultimi anni la materia penale dell'informatica impone una strategia di razionalità nel sistema delle fonti. Se da un lato la legislazione si muove nella traiettoria di rispondere con norme punitive incriminatrici sempre più rigorose, d'altro lato si registra una disseminazione delle fonti in vari testi legislativi che compromette la configurazione di un assetto sistematico della materia. L'interprete è chiamato a muoversi in un orizzonte normativo sempre più ampio e complesso, caratterizzato anche da nuovi beni giuridici oggetto di tutela che allo stato sembrano tenuti insieme dal nuovo assetto che fa capo alla cybersicurezza. Appare, dunque, necessario ricomporre il quadro normativo progettando un testo legislativo autonomo che riconduca sotto un comune denominatore le numerose fattispecie di reato, conferendo coerenza sistematica alla nuova materia foriera di ulteriori sviluppi.

Cybersicurezza – Reati informatici – Sistemi informatici – Dati digitali – Testo unico

The project for an independent regulatory framework for the security of information systems and data

The regulatory complexity that has affected cybercriminal law in recent years requires a strategy of rationalization in the system of sources. While legislation is moving toward responding with increasingly stringent punitive criminal provisions, there is also a dissemination of sources across various legislative texts, compromising the creation of a systematic framework for the subject. Interpreters are required to navigate an increasingly broad and complex regulatory landscape, also characterized by new legal assets subject to protection that currently appear to be held together by the new framework centered on cybersecurity. It therefore appears necessary to restructure the regulatory framework by designing a separate legislative text that brings together the numerous types of crimes under a common denominator, lending systematic coherence to this new field, which promises further developments.

Cybersecurity – Computer crimes – Information systems – Digital data – Consolidated law

L'Autore è professore associato di Diritto penale presso il Dipartimento di Giurisprudenza dell'Università degli Studi Federico II di Napoli

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement - Parte 1*, a cura di Gaetana Morgante e Gaia Fiorinelli

Sommario: 1. Mettere a fuoco le questioni aperte: *quid iuris*? – 2. Il bisogno crescente di protezione. – 3. I valori e i beni giuridici emergenti da tutelare. – 4. Per una decisa svolta dommatica. – 5. Da dove cominciare? La necessità di un Codice autonomo.

1. Mettere a fuoco le questioni aperte: *quid iuris*?

Questa mattina[1] cominceremo con il fare il punto della situazione su una nuova materia dove il gius-penalista si trova a navigare a vista in un oceano di fonti del diritto di varia natura e collocate su diversi livelli gerarchici. Questo variegato assetto disciplinare impone un intervento di armonizzazione con i principi di governo della materia penale, la cui prospettiva dommatica è chiamata a confrontarsi con strutture normative altamente volatili e con l'intervento regolatore del diritto positivo che si presenta sempre *a-sincrono* rispetto alle vicende tecnologiche che evolvono rapidissimamente e condizionano il bisogno di tutela[2].

L'attenzione del giurista è oggi rivolta a una nuova forma di diritto, un diritto che si forma in divenire, incontrollabile, collocato oltre le fonti della legislazione ordinaria, un diritto spesso autoprodotto come accade per le autonome discipline di regolazione dei comportamenti in Rete adottate dai grandi motori di ricerca. E poi, le scelte selettive dei provider che limitano il diritto degli utenti alla libera navigazione e controllano e selezionano le informazioni da introdurre in Rete sotto le forme di interventi normativi, prescrittivi, vincolanti per gli utenti[3].

I precetti delle norme penali di questo moderno ambito sfidano il limite di legittimità della norma penale in bianco, poiché vi sono molte figure di reato che attendono l'integrazione della descrizione della condotta vietata da altre norme di rango inferiore, entrate nella loro vigenza anche in epoca successiva[4]. Si tratta di una tecnica legislativa certamente opportuna per condotte che ancora non sono prese in considerazione dalla norma penale da integrare, ma che comunque pongono seri problemi per il cittadino circa la piena conoscibilità del precetto vietato e la prevedibilità della

1. Questo testo è la rielaborazione della Relazione tenuta in Pisa alla Scuola Superiore Sant'Anna il 16 giugno 2025 presso il Dipartimento di Giurisprudenza nell'ambito del Convegno: "*Dal Cybecrime alla Cyberwar: presentazione intermedia dei risultati del WP4 del progetto CyberRights-SERICS*".
2. Pica 1999; Parodi–Sellaroli 2020.
3. Zeno-Zencovich 2003; Rodotà 2010, p. 337; Allegri 2016, p. 8.
4. Amato Mangiameli–Saraceni 2019.

responsabilità che ne dovesse derivare per la loro violazione.

Se lo schema originario vedeva la scelta di politica criminale, intesa come uno degli strumenti della politica sociale rivolta al contrasto al crimine, questa volta il paradigma è mutato. Occorre progettare una politica criminale a base tecnologica, una disciplina che integri saperi diversi e che collaborino all'opera di prevenzione e poi di repressione nel contrasto al crimine tecnologico, prendendo atto che gli attori sulla scena non sono più soltanto il criminale, il giudice, la prigione, ma accanto a questi si ritrovano oggi nuovi attori istituzionali e professionalità inedite in campo penale[5].

Il vecchio paradigma, infatti, guardava alla relazione tra persone e poi tra persone e soggetti (anche non fisici – persone giuridiche), oggi occorre guardare a una relazione tra soggetti fondata su un diaframma, un legame intermedio, uno strumentario di natura tecnologica, la cui portata deve essere valutata in termini di relazione complessa, dove non esiste un autore del crimine bensì un apparato tecnico o un'infrastruttura immersi nella immaterialità della condotta; una platea di soggetti offendibili di natura vulnerabile per essere anche sotto-dotati tecnologicamente; una giustizia penale che oltre ai codici è chiamata a utilizzare mezzi altamente sofisticati per accertare i fatti; un processo penale la cui lunghezza può lasciare insoddisfatti i danneggiati se non si dota di un contesto tecnologico oltre che tecnico-giuridico che offra tempestività ed effettività alla decisione[6].

Il tema ha raggiunto una tale dimensione che il penalista tradizionale perde di vista il "fatto reato", la sua articolazione costitutiva, la sua rilevanza sociale, e prende atto che la sua analisi deve affrontare fenomeni di massa, danni a interessi giuridicamente qualificati che riguardano un numero indefinibile di individui – i c.d. reati a soggetto passivo diffuso –; illeciti commessi su un territorio senza confini; identificazione dei responsabili le cui tracce si disperdono in un universo immateriale[7]. L'indagine probatoria per l'accertamento del reato si depotenzia nell'attraversare percorsi che non sono più di semplice constatazione di una circostanza concreta, ma di un apprezzamento che passa per le maglie di discipline tecniche anche diverse da quella giuridica. La prova biologica del DNA divenuta la regina nei reati di sangue viene sostituita nei reati informatici dalla prova tecnologica della produzione e dell'uso del dato digitale.

Anche da un punto di vista didattico occorre aprire gli occhi ai giovani studenti su questo nuovo mondo, destinato a introitare rapidamente il vecchio, insegnando che le regole del vecchio non sono più sufficienti e adeguate a comprendere il nuovo e ricomporre un ordine conferente alle sue caratteristiche.

Anche la categoria della c.d. "quarta rivoluzione industriale" appartiene al lessico di un modello tradizionale, superato, di considerare il rapporto uomo-macchina[8]. Oggi è necessario guardare a un rapporto rovesciato macchina-uomo, non solo perché la macchina si sostituisce all'uomo seguendo la progettazione dell'uomo, ma perché la macchina tende a divenire indipendente dall'uomo e l'uomo è destinato a intervenire solo per correggere o arginare l'azione dei meccanismi tecnologici che compongono una nuova macchina: dal Web 2.0 con interazione tra gli utenti al Web 4.0 con la prevalente operatività dell'Intelligenza Artificiale[9]. La frontiera è la difesa dell'uomo e delle sue libertà rispetto alle iniziative di una "macchina pensante".

Ecco, dunque, che il vasto panorama dei regimi regolativi è talmente ampio e variegato che con la sola esegesi svolta sull'attuale assetto normativo con la disseminazione in vari testi legislativi si rischia di prospettare in maniera caotica e confusa la materia, per cui anche la ricerca di un ordine sistematico dotato di intrinseca razionalità va svolta con rigore ed equilibrio.

5. Picotti–Salvadori–Flor (s.d.), p. 5.
6. Sisto 1985, p. 28.
7. Cadoppi–Canestrari–Manna–Papa 2023.
8. Mantovani 1968; Rodotà 1973.
9. Si tratta della fonte base dettata dal Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024. Il quadro delle fonti del diritto si è completato con la legge n. 132 del 23 settembre 2025 che regola l'uso dell'Intelligenza Artificiale in Italia.

2. Il bisogno crescente di protezione

L'istanza di protezione rivolta al diritto penale deve prendere atto che occorre introdurre un presidio di tutela penale a struttura funzionale composita: da un lato la *Cybersecurity*, vista come difesa del complesso tecnologico, vale a dire dei sistemi e delle strutture informatiche dagli attacchi ostili provenienti dall'esterno; dall'altro la *Sicurezza informatica*, vale a dire la protezione delle informazioni e dei programmi per il loro trattamento[10].

In generale appare più congruente ridefinire la materia come quella della "Sicurezza informatica e dei dati" per compendiare gli entrambi assetti di tutela che meritano una sinergica regolazione giuridica di prevenzione e repressione.

Gli attacchi informatici provenienti dall'esterno – *cyber* attacchi – vengono realizzati con appositi programmi ostili definiti *malware* che analizzano e sfruttano la vulnerabilità dei sistemi informatici e, in questo modo, l'abuso della tecnologia informatica ai fini di profitto illecito può portare alla consumazione di reati che vanno a comporre la classe dei *cybercrimes*.

La punta estrema di questo nuovo modo di sviluppare un moderno conflitto è la *cyberwar*, un modo diverso di manifestare ostilità, in cui l'iniziativa offensiva viene sempre portata nell'ombra della difficile identificazione dei responsabili e dove il destinatario ha la necessità di difendersi con gli stessi mezzi e, anzi, mettere in campo sempre nuove e più aggressive armi tecnologiche.

Questa è la ragione per cui, diversamente dal mondo reale, c'è bisogno di forme di tutela differenziata per la difesa dalle ostilità informatiche, una tutela tecnologica e una tutela giuridica che svolgano simultaneamente quella funzione preventiva e punitiva[11].

La realtà insegna che nella finalità degli attacchi è insita la sottrazione o il rendere temporaneamente indisponibili le informazioni di archivio e le operatività delle risorse informatiche in settori nevralgici della società, quali quello commerciale, strategico, militare, sanitario, per ottenere un profitto illecito. Sul piano del danno si stima, infatti, che queste pratiche illegali sempre più diffuse hanno registrato negli ultimi anni un peso economico su scala mondiale di oltre 2000 miliardi di dollari.

Per raggiungere questi obiettivi vengono elaborati sofisticati programmi detti *ransomware*, un tipo di *malware*, applicazione malevole, che viene progettata per infettare il sistema colpito e in questo modo estorcere denaro con il sequestro (blocco dei dati o del sistema) e la criptazione dei file. Si sono registrati nel corso degli ultimi cinque anni attacchi alla Campari (con riscatto richiesto di 15 milioni di dollari nel 2020); Enel (due attacchi nel 2020, nel secondo il ransomware NetWalker ha usato la *tecnica della doppia estorsione*, dopo aver rubato circa 5 tb di dati ha minacciato di renderli pubblici qualora non fosse stato pagato il riscatto di 16 milioni di dollari); Bonfiglioli (2019); Zambon (2020); Geox, Luxottica, Agenzia Territoriale per la Casa di Torino (2021); Comune di Brescia (2021); fino al caso più clamoroso della Regione Lazio, colpita a inizio agosto 2021.

Va subito posto in evidenza che il tema sul piano generale sta acquisendo una configurazione a cerchi concentrici: la gestione politica del settore; la gestione tecnica e la difesa *dei* sistemi informatici; la protezione della persona *dai* sistemi informatici; l'automazione e la responsabilità dei sistemi di Intelligenza Artificiale.

L'idea di tutela dei cerchi concentrici detta le coordinate delle varie competenze sul campo: il primo riguarda le scelte politiche trans-nazionali, come la tutela della libertà e della democrazia; il secondo concerne la complessiva disciplina legislativa nazionale; il terzo tiene conto della disciplina penale come specifico ambito di tutela.

A proposito della tutela penale non si può prescindere dal primo atto sovranazionale che ha coinvolto i singoli stati aderenti, la *Convenzione Cybercrime di Budapest del 2001*, che per la prima volta ha regolato in maniera comune alcune ipotesi

10. Si veda la Comunicazione congiunta al Parlamento europeo e al Consiglio dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, *Resilienza, deterrenza e difesa: verso una cybersicurezza forte per l'Ue*, 13 settembre 2017.
11. A livello di disciplina eurounitaria si veda il Regolamento del Parlamento europeo e del Consiglio 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), adottato l'11 luglio 2022.

di illecito chiamate ad assumere rilevanza penale in tutti i Paesi sottoscrittori[12].

Questa prima regolazione a livello internazionale ha fatto emergere la necessità di elaborare due distinte categorie normative in campo penale: a) i sistemi informatici quali beni o oggetti di tutela penale; b) i sistemi informatici quali strumenti di commissione dei reati che compaiono come elementi costitutivi della fattispecie incriminatrice[13].

In questo modo assume particolare rilevanza la trasmigrazione della materia informatica dalla categoria dei servizi a quella dei beni, per cui occorre indirizzare la progettualità verso una autonoma e indipendente collocazione sistematica della relativa disciplina penale.

Va sottolineato, peraltro, che in tutti gli interventi legislativi degli ultimi anni, al di là della individuazione di un bene ideale di riferimento, resta al centro dell'interesse del diritto penale e della stesura delle diverse fattispecie incriminatrici uno specifico e ricorrente oggetto materiale del reato. Alla base di tutto il complesso quadro normativo che sta via via delineandosi, infatti, compaiono i sistemi informatici da una parte e i dati digitali o informatici dall'altra, come elementi costitutivi della sicurezza informatica.

3. I valori e i beni giuridici emergenti da tutelare

Nella progettazione normativa degli assetti di tutela non si può non partire dalla persona, identificata da Rodotà in corpo fisico e corpo elettronico, portatrice di interessi specifici: onore, reputazione, riservatezza informatica, sicurezza informatica, proprietà intellettuale, domicilio informatico, genuinità dell'informazione (versus *fake news*).

Ecco perché si impone l'individuazione di un bene giuridico di categoria di nuovo conio, del tutto diverso e onnicomprensivo rispetto alle categorie tradizionali che la dottrina ha utilizzato finora, come ad esempio la riservatezza (*la privacy*) desumendola dalle norme di valore dall'art. 14 Cost. – sulla segretezza della corrispondenza – e dall'art. 15 Cost. – sul domicilio informatico –, e, a livello di regolazione sovranazionale continentale, dal principio di democrazia[14].

Il fulcro dell'assetto di tutela rimane sempre e comunque la persona umana, la sua vita, la sua dignità, seppure con i suoi diritti e la sua operatività rifratta tra realtà concreta e realtà immateriale della Rete, ma da cui non è possibile prescindere in tutti i propositi di protezione di settori e materie che sono semplicemente funzionali al suo sviluppo e alla sua integrità e per nulla assoluti e autonomi[15]. E l'ordinamento giuridico è chiamato a consolidare un sistema di difesa del singolo nell'ambito della collettività in termini di solidarietà umana.

Il passaggio successivo è costituito dalla tutela dei beni funzionali: primo fra tutti il patrimonio, sia in quanto componente informatica sia come finalità di profitto della condotta, oltre a segmenti di mercato, assetti tecnologici, infrastrutture tecniche ed altro[16].

La lesione di questi beni determina, non solo un danno al titolare dell'interesse, ma un rilevante danno reputazionale per le aziende che in questo modo si presentano vulnerabili sul mercato. Senza tenere conto dei sensibili rischi e nocumento per la propria clientela, come accaduto recentemente nel caso di Intesa San Paolo a Bari con accesso abusivo e sottrazioni massive di informazioni sensibili della clientela.

Esaminando il caso dalla prospettiva teleologica in materia penale si tratta di interessi di una categoria composita, dove a emergere non è un singolo bene bensì un "luogo di tutela", in perfetta analogia con il concetto di pubblica economia, anch'esso ampio campo di tutela con interessi differenziati che lo compongono.

12. La cui attuazione nel nostro ordinamento è avvenuta con la legge n. 48 del 18 marzo 2008.
13. Si veda a tale proposito il Disegno di legge 2773 Ministro di Grazia e Giustizia, XI legislatura Camera dei Deputati, secondo il quale le nuove fattispecie criminose rappresentano semplicemente "… nuove forme di aggressione, caratterizzate dal mezzo o dall'oggetto materiale, ai beni giuridici (patrimonio, fede pubblica, ecc.), già oggetto di tutela nelle diverse parti del corpo del codice".
14. Rossato 2014, p. 21.
15. Picotti 2013.
16. Pecorella 2006.

In realtà, in termini di assetto di tutela si prende atto della necessità di apprestare protezione alla sicurezza del settore informatico cogliendo gli stessi profili teorici della tutela dei beni comuni, come avviene per l'acqua, le matrici ambientali. La gestione svolta in maniera non egoistica di un macro-bene, bensì in forma collettiva, dove appunto quella gestione collettiva va a coincidere con la forma di protezione.

Si assiste in questo modo a una prima svolta importante. L'utente non è più tale, ma diventa consumatore, acquisendo i profili identificativi e qualificativi della vittima: si pensi alla profilazione anagrafica, la profilazione professionale, la profilazione sanitaria, ecc.

Da qui la considerazione della posizione di vulnerabilità implicita del soggetto, il quale si trova in quella posizione, per il solo fatto di navigare in Rete, di chi agisce sulla base di un suo consenso presunto, di un consenso non espresso esplicitamente e formalmente, ma indirettamente per il fatto di trovarsi in Rete e sulla base di questa qualificazione viene riconosciuto dagli altri utenti e profilato in modo da essere identificato, seppure non abbia ceduto espressamente il proprio profilo identificativo con il suo consenso.

4. Per una decisa svolta dommatica

Per la sicurezza del settore informatico la dommatica tradizionale deve essere necessariamente rivisitata in ragione delle peculiarità del nuovo ambito normativo. A partire dal concetto di *Cyberspazio* che non ha un territorio di riferimento dove si consumano reati e, dunque, non radica una competenza processuale sempre agevolmente definibile, perché diventa difficile stabilire le coordinate di consumazione del fatto reato a seconda dell'evento o della condotta [17]. Il concetto di libertà di agire che è alla base della fisiologia dell'ecosistema della Rete vede come suo corrispettivo l'autodeterminazione ad agire in ambiti territoriali sempre diversi.

Le note questioni di un controllo preventivo o successive da parte dei provider nel caso *Vividown c. Google* hanno segnato un momento importante per individuare le posizioni di controllo e garanzia in capo alle società che forniscono servizi in Rete e per essi alle persone fisiche le rappresentano[18].

Ma non basta. Occorre ripensare a tutta la dommatica, ai principi di orientamento della materia penale, per adattare ad essa la nuova classe di reati, ripensando all'introduzione di "buone pratiche" legislative per metterla in sincronia con quelle vigenti e allestire nuove ipotesi di reato, puntuali, precise, definite, effettive, pronte ad essere utilizzate dal giudice[19]. Un novero di reati che si caratterizza per le particolari modalità di realizzazione della condotta e per lo strumentario tecnologico in uso nel mondo dematerializzato della Rete che si risolve nella precisione della norma penale come verifica in sede processuale.

Sul piano della struttura del fatto-reato la prima considerazione investe la natura della condotta. Si tratterà di descrivere solo reati di azione, sembrerebbe, confinando il caso dell'omissione colpevole alla regola degli obblighi giuridici dell'art. 40 cpv c.p.

Come valutare e individuare, poi, la causa determinante o la contemporanea esistenza di altre cause che hanno dato vita all'evento facendo ricorso a una disciplina datata al 1930 che già con il banco di prova del disastro innominato non ha fornito adeguate risposte. E in questo caso come può giocare l'incidenza della causa individualizzante sul piano statistico di probabilità e possibilità nell'ottica fornita dalla sentenza Franzese? In questo ambito la relazione causa/effetto come va intesa, dal momento che se nella realtà concreta si può raggiungere un ragionevole grado di certezza,

17. Perusia 2001, p. 1835. Più recentemente la Suprema Corte su rinvio pregiudiziale del Tribunale di Perugia ha dettato un importante principio di diritto sulla questione, in Cass. pen., Sez. III, Sent. n. 38511 del 18 settembre 2024, "L'unico parametro di riferimento applicabile è perciò quello di cui al comma 3 dell'art. 9 cod. proc. pen., a tenore del quale la competenza per territorio 'appartiene al giudice del luogo in cui ha sede l'ufficio del pubblico ministero che ha provveduto per primo a iscrivere la notizia di reato nel registro previsto all'art. 335'".
18. Ci sia consentito rinviare a Troncone 2014, p. 2060.
19. Secondo le coordinate tradizionali della materia penale, in Fiandaca–Musco 2019, p. 43: "…in altri termini assurge a bene giuridico soltanto quell'interesse, o quell'accorpamento di interessi, idonei a realizzare un determinato scopo utile per il sistema sociale o per una sua parte". Sull'assetto delle figure di reato di parte speciale in ordine alla tutela di funzioni, si rinvia a Moccia 1995, p. 344.

nel caso della Rete diventa difficile sceverare tra le tante cause che intervengono e si affiancano a quella iniziale e forse perdono vigore per effetto di quelle sopravvenute, queste ultime saranno da reputare sempre eccezionali? Né va escluso il tema del concorso di persone che non si pone soltanto nella prospettiva della individuazione dell'azione oggettivamente svolta, ma soprattutto per la necessità che le indagini giudiziarie abbiano come obbiettivo l'accertamento probatorio di tutti i contributi alla consumazione del reato.

L'evento. In senso naturalistico o sarà da intendere in senso giuridico come sembra suggerire il contesto dematerializzato in cui prende ragione? Tra le pieghe della valutazione del fatto non può mancare il riferimento all'elemento soggettivo e da qui il dilemma se, ai fini risarcitori, va considerato il rischio sociale della navigazione in Rete che qualunque utente dovrà considerare nel momento in cui ne fa accesso, e la rilevanza della colpevolezza a chiudere il cerchio dell'accertamento della responsabilità penale.

Sul piano della risposta punitiva occorre tenere nella debita considerazione anche la responsabilità amministrativa degli enti del d.lgs. n. 231/2001[20]. Soprattutto armonizzando le cause estintive del reato di natura premiale o deflattiva con la legislazione di settore, valorizzando la riabilitazione dell'ente alla luce degli interventi correttivi conformi alle leggi, di *compliance*.

Il vero problema però resta quello di valorizzare gli scudi protettivi per le vittime come ci indirizzano le fonti europee, bersagli di danni che non sempre è possibile qualificare con parametri econometrici.

Esiste inoltre lo scottante problema della permanenza degli eventi dannosi in Rete e, per questo, ipotizzare reati a consumazione prolungata o si tratta soltanto di effetti persistenti di un reato a consumazione istantanea?[21] Come nella corruzione?[22]

Possono permanere in Rete senza soluzione di continuità i patrimoni informativi di persone decedute, i cui eredi non sempre hanno competenza e capacità tecnologiche per gestire la correttezza di quelle informazioni[23]. È possibile ipotizzare l'istituzione di un'Autorità in Rete chiamata a gestire i patrimoni informativi dispersi che potrebbero offendere la memoria dei trapassati?

Le perplessità sono tante, come si vede, e non aiutano gli esempi che quotidianamente registriamo nei vari tribunali territoriali, come quello della richiesta di archiviazione avanzata dalla Procura di Torino di qualche mese fa in ordine a un caso di diffamazione in Rete, sventata dall'intervento correttivo del GIP[24]. Chissà perché, secondo il PM delle indagini, la dematerializzazione dovrebbe depotenziare il contenuto offensivo di espressioni che ledono la reputazione di una persona, e non ritenere che l'effetto moltiplicatore del rimbalzo le rende ancora più cariche di lesività! E cosa penseranno i figli e gli eredi quando leggeranno in Rete frasi e contenuti non rettificati, non è quello un danno che prende vita dal riflesso indiretto dell'originario primo danno?

E poi come è possibile trattare la punibilità di una fonte infettiva, di un *malware* che si propaga in un *device* e si diffonde in Rete? In questo caso occorrono gli ingegneri ad accompagnare il legislatore e prevedere in maniera inequivocabile l'appropriata terminologia da utilizzare, forse con una tabella integrativa della legge come è avvenuto con il d.p.r. n. 309/90 in materia di stupefacenti.

Il punto più oscuro resta però quello della effettività della pena, quale può essere la risposta punitiva in termini di rieducazione aderente a quel tipo, alla natura di quel reato? Forse le c.d. pene tecnologiche e quali?

E le misure cautelari reali come vanno congegnate? E le pene o le misure tecnologiche inabilitative, come spesso si è sentito del c.d. "ergastolo

20. Fondaroli 2019; Monti 2022.

21. Si ricorda che la giurisprudenza è ferma, alla luce della norma vigente, a ritenere la diffamazione con il mezzo del Web un reato di natura istantanea che non diviene permanente per gli effetti persistenti dell'offesa in Rete, come stabilisce Cass. pen., Sez. V, Sentenza n. 32533 dell'11 luglio 2025.

22. Aimi 2020.

23. Marseglia 2025.

24. Tribunale di Torino, Ufficio del GIP, ordinanza del 14 gennaio 2025, in "Giurisprudenza penale" (online), 20 gennaio 2025.

informatico", come vanno irrogate e controllate? L'esperienza del braccialetto elettronico per le misure alternative ci fornisce spunti di esperienza importanti per comprendere la fallibilità di un sistema tecnologico che non si mostra ancora all'altezza delle sfide da affrontare.

Infine, quale risposta indennitaria per la vittima in permanente minorata difesa tecnologica?

Va ricordato a tale proposito che la nuova legge sull'Intelligenza Artificiale n. 132 del 2025, però esclusivamente per le ipotesi di reato in essa contenute, ha introdotto una nuova specifica aggravante con il n. 11-*decies* all'art. 61 c.p. sulla minorata difesa della vittima.

5. Da dove cominciare? La necessità di un Codice autonomo

Riteniamo sia giunto il momento di dare vita a un'esperienza legislativa destinata a sciogliere tutti i nodi sistematici di questa complessa materia che acquista progressivamente una sempre maggiore ampiezza mettendo in campo un corpo normativo unico che potrebbe assumere la denominazione di "Codice per la sicurezza informatica e dei dati".

In questo modo si darebbe valore a una nuova area di tutela penale racchiusa nella denominazione cybersicurezza, dove il comune denominatore è costituito dai mezzi informatici e i dati digitali che le danno vita.

La prassi applicativa degli ultimi anni registra preoccupanti crepe interpretative dovute alle asincroniche simmetrie tra tecnologia in evoluzione e disciplina giuridica in costante ritardo che spinge l'opera dei giudici verso una giurisprudenza creativa oltre il rigido testo normativo. In questo modo si evidenziano i limiti di una legislazione improvvisata e sprovvista dal suo nascere di un criterio organizzativo sistematico che fornirebbe la chiave di lettura a soluzioni coerenti[25]. L'opera legislativa, purtroppo, si attesta sull'esigenza di dettare norme secondo la necessità contingente priva di una strategia di lunga durata, inserendo nuove figure di reato o innumerevoli aggravanti in norme penali già esistenti sotto i più diversi interessi giuridici di categoria che frammentano sempre di più il contesto della materia.

Occorrerebbe invece richiamare l'impegno deontologico del legislatore nella cura della legge, verso una formulazione anche lessicale che non debba lasciare margini al dubbio nei destinatari in termini convenzionali di prevedibilità della condanna, e nel giudice chiamato ad applicarla con sufficiente precisione[26].

Va ricordato che diversamente dal passato è stato dettato un vincolo normativo al legislatore con l'art. 3-*bis* c.p., "Principio della riserva di codice", vale a dire l'obbligo di disciplinare in modo organico fattispecie incriminatrici appartenenti a una stessa materia[27]. Una materia che va individuata sulla base del comune denominatore intorno al quale strutturare il precetto e che trova il suo punto di qualificazione giuridica, il suo comune denominatore di principio, appunto, nella "Sicurezza informatica e dei dati".

Da un punto di vista della tecnica normativa occorre fare leva sull'art. 15 del codice penale, "Materia regolata da più leggi penali o da più disposizioni della medesima legge penale", e mettere in campo figure di reato, seppure nel *genus* già esistenti nella legislazione, nella *species* distinte per elementi specializzanti, come si è proceduto – forse in maniera sovrabbondante – con il delitto di danneggiamento dell'art. 635-*bis* c.p. e non come avvenuto con l'introduzione del terzo comma dell'art. 629 c.p. che punisce l'estorsione informatica non come una semplice circostanza ma come una autonoma ipotesi di reato.

Un Testo Unico coordinato sotto la denominazione di un nuovo catalogo di reati eviterebbe i continui rinvii sistematici che gli attuali testi contengono, sottraendo omogeneità e coerenza alla normativa di settore.

Peraltro, seguendo l'esempio delle direttive dell'Unione europea, sarebbe addirittura

25. Posizione più volte ribadita, tra gli altri, da Fumo 2013, p. 775: "Forse anche per questo – muovendosi in un'ottica di stampo contenutistico – il legislatore ha ritenuto di non varare un corpus unitario di (nuove) norme repressive, ma ha scelto di prevedere le 'nuove condotte criminali' (se non tutte, almeno le più rilevanti), collocandole 'topograficamente' negli habitat normativi che sembravano – di volta in volta – più opportuni. Non sempre si è trattato però di scelte felici"; Picotti 2020, p. 709.
26. Viganò 2025.
27. Donini 2018.

auspicabile una sinossi normativa in apertura del provvedimento, contenente la esatta definizione dei vari requisiti e dei concetti come elementi di tipicità contenuti nelle diverse figure di reato.

Ad esempio, non è sempre chiaro in quale modo il legislatore declini il concetto di vantaggio, cosa diversa dal profitto, eppure utilizzato indifferentemente, come nel caso della finalità ulteriore a quella esclusivamente economica nel furto[28].

Con questo indirizzo non vi sarebbe stato alcun problema nel ritenere infondata la qualificazione normativa di una semplice SIM in quella di apparato telefonico, nessuna assimilazione per analogia sarebbe stata mai ipotizzata a partire dal terreno tecnologico oltre che giuridico, nodo sciolto invece nel 2024 con una pronuncia della Suprema Corte di Cassazione[29].

Attualmente, invece, assistiamo a degli innesti normativi di nuove fattispecie nelle classi di reato tradizionali e di parti di norme nei precetti preesistenti che non sempre mostrano una decisiva coerenza: delitti contro la libertà morale, contro l'inviolabilità del domicilio, contro l'inviolabilità dei segreti, contro il patrimonio.

Ad esempio, il c.d. *revenge porn* o meglio la "Diffusione illecita di immagini o video sessualmente espliciti" dell'art. 612-*ter* c.p. è una forma di trattamento illecito di dati personali, è violazione della riservatezza, e tuttavia non si trova nel Codice del trattamento dei dati personali perché in apertura dell'art. 167 CdP vi è una clausola di sussidiarietà espressa che lo esclude[30]. Su questa scia si pone la nuova figura di delitto di "Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale" introdotta con l'art. 612-*quater* c.p. dalla legge n. 132 del 2025 consistente nella manipolazione di dati nota come *deepfake*.

A ben vedere, si tratta del medesimo fatto, con le medesime modalità di realizzazione, sebbene con un diverso disvalore il che implica che il disvalore autonomo dell'art. 167 CdP ha ceduto il passo e viene dequalificato solo per ragioni di misura della pena.

A titolo di pura esemplificazione va segnalata la profonda interrelazione tra i delitti degli artt. 615-*ter* "Accesso abusivo ad un sistema informatico" e 615-*quater* "Detenzione, diffusione e installazione abusiva di apparecchiature, codici e latri mezzi atti all'accesso a sistemi informatici o telematici" del codice penale e quello previsto nel Codice del trattamento dei dati all'art. 167-*bis* "Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala" che sembra replicarne i caratteri seppure armonizzati con una clausola di sussidiarietà espressa.

Ad esempio, il campo patrimoniale delle criptovalute vede nei loro meccanismi di funzionalità un trattamento di dati non personali, contenuti nelle due chiavi informatiche che ne regolano la titolarità. Non c'è uno scambio di valuta bensì uno scambio di dati che coincide con uno scambio di valori economici. Andrebbe, dunque, ipotizzata una disciplina specifica nel campo informatico, per assicurare la stessa tutela che il codice penale riserva alla moneta ufficiale in corso, prima la lira oggi l'euro.

Su questo tema si agita senza sicuri approdi la giurisprudenza degli ultimi anni, non avendo il legislatore regolato al pari delle monete virtuali il regime giuridico della circolazione delle criptovalute e il criterio di valorizzazione attribuito dal mercato, marcandola soltanto a fini fiscali quale forma di accumulazione della ricchezza e rendendo in questo modo anche ardua l'applicazione di tutte le ipotesi di sequestro penale degli artt. 240 e ss. c.p. finalizzati alla confisca[31].

In definitiva, le condotte di sopraffazione della criminalità in questo settore sono particolarmente pervasive e insidiose, peraltro attivate in uno spazio indistinto che si scontra con i nostri strumenti di tutela tradizionali che alla base registrano spazi

28. Cass. SS.UU. pen., Sent. n. 41570 del 25 maggio 2023.
29. Cass. pen. Sez. VI, Sent. n. 42941 dell'11 settembre 2024, che ha dichiarato illegittimo estendere la norma dell'art. 391-*ter* c.p., che vieta l'introduzione di apparecchi telefonici cellulari in carcere, anche alla scheda SIM, negandone la natura di "dispositivo mobile".
30. Correra–Martucci 1986.
31. Corasaniti 2012, p. 819. Così come anche previsto all'art. 30 – *Abusivismo – della Legge sui mercati delle cripto-attività*, d.lgs. n. 129 del 5 settembre 2024.

finiti, confini certi, elementi identificativi concreti e incontrovertibili[32].

Occorre, dunque, ricalibrare in termini moderni il catalogo "dei delitti e delle pene" di questa materia, destinato a confrontarsi con una nuova e diversa realtà, quella immateriale, e che, nostro malgrado, invoca nuove mappe e coordinate di navigazione per la salvaguardia delle nostre libertà.

Riferimenti bibliografici

A. Aimi (2020), *Le fattispecie di durata. Contributo alla teoria dell'unità o pluralità di reato*, Giappichelli, 2020

A. Alessandri (1990), *Criminalità informatica*, in "Rivista trimestrale di diritto penale dell'economia", 1990

M.R. Allegri (2016), Riflessioni e ipotesi di costituzionalizzazione del diritto di accesso a Internet, in "Rivista AIC", 2016, n. 1

A.C. Amato Mangiameli, G. Saraceni (2019), *I reati informatici. Elementi di teoria generale e principali figure criminose*, Giappichelli, 2019

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

G. Corasaniti (2012), *Brevi note in tema di confisca obbligatoria di beni e strumenti di commissione dei reati informatici alla luce della legge 15 febbraio 2002 n. 12*, in "Diritto dell'informazione e dell'informatica", 2012

M. Correra, P. Martucci (1986), *I reati commessi con l'uso del computer. Banche dati e tutela della persona*, Cedam, 1986

M. Donini (2018), *La riserva di codice (art. 3-bis cp) tra democrazia normante e principi costituzionali. Apertura di un dibattito*, in "La legislazione penale", 20 novembre 2018

G. Fiandaca, E. Musco (2019), *Diritto penale. Parte generale*, Zanichelli, 2019

D. Fondaroli (2019), *La responsabilità di persone giuridiche ed enti per i reati informatici ex D.Lgs. n. 231/2001*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), "Cybercrime – omnia – Trattati giuridici", Utet, 2019

M. Fumo (2013), *La condotta nei reati informatici*, in "Archivio penale", 2013

F. Mantovani (1968), *Mezzi di diffusione e tutela dei diritti umani*, in "Archivio giuridico", 1968

R. Marseglia (2025), Privacy *e tutela dei dati personali* post mortem, Esi, 2025

S. Moccia (1995), *Dalla tutela di beni alla tutela di funzioni: tra illusioni e riflussi illiberali*, in "Rivista italiana di diritto e procedura penale", 1995

A. Monti (a cura di) (2022), *Cybercrime e responsabilità da reato degli enti. Prevenzione e modello organizzativo e indagini preliminari*, Giuffrè, 2022

C. Parodi, V. Sellaroli (a cura di) (2020), *Diritto penale dell'informatica. Reati della rete e sulla rete*, Giuffrè, 2020

C. Pecorella (2006), *Diritto penale dell'informatica*, Cedam, 2006

E. Perusia (2001), *Giurisdizione italiana anche per le offese on line su un sito straniero*, in "Cassazione penale", 2001

32. Alessandri 1990.

G. Pica (1999), *Diritto penale delle tecnologie informatiche*, Utet, 1999

L. Picotti (2020), *Cybercrime e diritto penale*, in C. Parodi, V. Sellaroli (a cura di), "Diritto penale dell'informatica. Reati della rete e sulla rete", Giuffrè, 2020

L. Picotti (2013), *Tutela penale della persona e nuove tecnologie*, Cedam, 2013

L. Picotti, I. Salvadori, R. Flor (s.d.), *Reati informatici, riservatezza, identità digitale*, in "www.aipdp.it", s.d.

S. Rodotà (2010), *Una costituzione per Internet?*, in "Politica del diritto", 2010

S. Rodotà (1973), *Elaboratori elettronici e controllo sociale*, il Mulino, 1973

A. Rossato (2014), *Sulla natura dei beni comuni digitali*, in A. Pardi, A. Rossato (a cura di), "I beni comuni digitali. Valorizzazione delle informazioni pubbliche in Trentino", Quaderni della Facoltà di Giurisprudenza, Trento, 2014

F.P. Sisto (1985), *Diritto penale dell'informatica e recupero dei modelli tradizionali*, in "Critica penale", 1985

P. Troncone (2014), Il caso *Google* (e non solo). Il trattamento dei dati personali e i controversi requisiti di rilevanza penale del fatto, in "Cassazione penale", 2014

F. Viganò (2025), *Chiarezza della legge e principi costituzionali*, in "Sistemapenale.it", 30 settembre 2025

V. Zeno-Zencovich (2003), *Informatica ed evoluzione del diritto*, in "Il diritto dell'informazione e dell'informatica", 2003

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0249 • articolo sottoposto a peer review • pubblicato in anteprima il 25 nov. 2025

Maria Vittoria Zucca

Mappare il *Crime-as-a-Service*: analisi delle strutture, dei ruoli e dei servizi nell'offerta criminale digitale

La presente ricerca si propone di indagare il fenomeno del *Crime-as-a-Service* (CaaS) quale modello consolidato di "industrializzazione" del crimine digitale. In risposta alle lacune individuate nella letteratura, lo studio segue un approccio metodologico lungo due direttrici: (i) l'analisi dell'ecosistema CaaS, nelle sue componenti strutturali, organizzative e sociali; (ii) la mappatura dei servizi offerti – di supporto diretto e indiretto – e dei modelli economici sottostanti. A seguire, i comuni denominatori ricavati verranno posti a confronto con le definizioni criminologiche tradizionali di criminalità organizzata e, attraverso la costruzione di un *network graph* concettuale, saranno messi in luce punti di convergenza, di divergenza e le aree di non-sovrapposizione tra i due paradigmi. L'obiettivo della ricerca è quello di fornire strumenti interpretativi utili alla comprensione teorico-criminologica, alla qualificazione giuridica e al più efficace contrasto del crimine digitale "organizzato".

Crime-as-a-Service – Mercati illeciti – Criminalità organizzata – Cybercrime – Criminologia digitale

Mapping Crime-as-a-Service: An analysis of structures, roles, and services in the digital criminal offering

This study investigates the phenomenon of Crime-as-a-Service (CaaS) as a consolidated model of digital crime "industrialization." In response to the gaps identified in the existing literature, the research adopts a methodological approach articulated along two main axes: (i) the analysis of the CaaS ecosystem in its structural, organizational and social dimensions; and (ii) the mapping of the services offered – both direct and indirect forms of support – and the underlying economic models. The common denominators emerging from this analysis are subsequently compared with the traditional criminological definitions of "organized crime" and, through the construction of a conceptual network graph, points of convergence, lines of divergence and areas of non-overlap between the two paradigms are highlighted. The aim of the study is to provide interpretative tools that can support theoretical-criminological understanding, legal qualification, and the more effective countering of digitally "organized" crime.

Crime-as-a-Service – Illicit markets – Organized crime – Cybercrime – Digital criminology

L'Autrice è dottoranda del Programma di Interesse Nazionale in Cybersecurity, affiliata presso la Scuola Superiore Sant'Anna di Pisa e la Scuola IMT Alti Studi di Lucca

La ricerca si inserisce nell'ambito del Progetto PNRR "Partenariato Esteso" PE 7 SERICS Security and Rights in the Cyber Space/ Spoke 1: Progetto CybeRights Codice identificativo: M4C2 11.3 - PE0000014 - CUPJ53C22003110001

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement - Parte 1*, a cura di Gaetana Morgante e Gaia Fiorinelli

1. Cenni introduttivi: la "mercificazione" del crimine digitale

Si premetta come le dinamiche che oggi contraddistinguono il crimine informatico[1] non rappresentano una rottura radicale rispetto ai paradigmi criminali "classici", bensì una loro trasposizione nell'ambiente digitale. Invero, già nel secolo scorso la teoria criminologica della scelta razionale[2], sulla scia degli studi economici di Becker[3], concepiva il comportamento criminale come il risultato di una valutazione utilitaristica del rapporto costi/benefici associati ad un'azione illecita rispetto a quella lecita. In tale prospettiva, l'agente criminale si comporta come un attore razionale, orientato a massimizzare i benefici (ad esempio, i profitti attesi da un'attività illecita) e, parallelamente, a minimizzare gli eventuali rischi (come l'identificazione, l'arresto e la condanna). Benché originariamente concepito per l'analisi della criminalità "terrestre", tale modello teorico risulta sorprendentemente attuale se traslato nel dominio digitale, ove le medesime logiche attoriali si ripresentano. La transizione verso l'ambiente cibernetico[4] ha infatti favorito un avvicinamento graduale alla carriera (cyber) criminale: una presa di coscienza delle potenzialità (quali versatilità, elusività e opportunità di guadagno) offerte dagli strumenti informatici, che ha indotto molti individui a valutare la convenienza dell'azione digitale illecita.

A ciò si sommi l'odierna facilità di accesso alle competenze necessarie per condurre attività cybercriminali: ciò che un tempo richiedeva elevate capacità tecnico-informatiche è oggi reso disponibile a un pubblico più ampio, grazie ai servizi offerti da reti criminali specializzate, attive sul

1. Sulla nozione di crimine informatico, qui richiamata in senso ampio, si vedano, *ex multis*, Fiorinelli 2023, Picotti 2011, Pecorella 2006.
2. Si v. Cornish–Clarke 1986, Clarke 1985, tra i primi a formalizzare in modo sistematico l'approccio della *rational choice* in ambito criminologico.
3. Si rimanda a Becker 1968, che, muovendo dal suo paradigma economico, re-interpreta il comportamento criminale.
4. Si rimanda a Gibson 1984, per la prima formulazione del concetto di "cyberspazio"; v. inoltre Castells 1996, per sviluppi socio-tecnologici del concetto stesso.

mercato illecito, che adottano modelli di business simili a quelli legittimi[5]. Si può affermare che la digitalizzazione abbia favorito una "industrializzazione" (e, al contempo, "democratizzazione"[6]) del crimine, tramite il fenomeno oggetto di questo studio: il c.d. *Crime-as-a-Service*[7] (da qui in poi, CaaS), espressione paradigmatica della mercificazione domanda-offerta del sapere criminale. Il CaaS consente infatti di esternalizzare competenze tecniche, offrendo servizi e/o strumenti (si pensi al noleggio di *botnet* o allo sviluppo di *malware*) a soggetti terzi, siano essi affiliati o semplici clienti[8], potenzialmente privi di specifiche abilità informatiche, ma parimenti con l'intento di accedere a profitti illeciti.

Ciò comporta una forte riduzione dei costi d'ingresso al "mercato" criminale (in termini di risorse, competenze e rischio) e, parallelamente, una minimizzazione dell'esposizione personale. La vendita di *tool* illeciti, infatti, invece del loro utilizzo "diretto" da parte dello sviluppatore, consente di diluire la responsabilità lungo la catena criminale e di aumentare l'opacità delle operazioni, riducendo la tracciabilità. Si assiste così a una prosecuzione delle logiche razionali di matrice beckeriana e cornishiana da cui si è partiti, per cui l'agire cyber-criminale assume ad oggi i tratti di un'impresa orientata alla convenienza, alla replicabilità e all'efficienza. In questa prospettiva, lo studio si propone di indagare il fenomeno del CaaS, analizzandone *in primis* le strutture organizzative e i servizi offerti, così da, *in secundis*, identificarne i tratti comuni e metterli a confronto con i caratteri della criminalità organizzata tradizionale, al fine di evidenziare convergenze, divergenze (nonché, zone d'ombra) tra i due paradigmi teorico-definitori.

2. Una mappatura del *Crime-as-a-Service*

L'immediato proseguo della trattazione prende atto dalla consapevolezza di una lacuna nella letteratura esistente, derivante dalla mancanza di un approccio sistematico alle diverse tipologie di servizi offerti nell'ambito del CaaS. Gli studi attuali, infatti, tendono a focalizzarsi su alcune forme particolarmente note, come il *Ransomware-as-a-Service* (RaaS)[9], inserito nella famiglia dei *Malware-as-a-Service* (MaaS), trascurandone altre parimenti significative. A ciò si sommi una seconda criticità: la mancanza di studi interdisciplinari in grado di integrare, in un'unica cornice analitica, gli aspetti tecnici e i profili socio-criminologici che caratterizzano i gruppi CaaS. Una comprensione più articolata del fenomeno risulta dunque necessaria per ricavare i comuni denominatori tra le varianti di CaaS e per costruirne una "mappatura" strutturata. Alla luce dei più recenti report istituzionali[10] e degli studi di settore, l'analisi procederà seguendo un duplice binario: (i) l'esame della struttura organizzativa del CaaS, comprensiva dei ruoli professionali coinvolti e delle connessioni sociali; (ii) l'analisi dei principali servizi offerti e dei modelli economico-commerciali ad essi associati.

5. Sul ruolo delle comunità online e dei *marketplace* nel facilitare l'ingresso nel cybercrime, si v. in particolare Lusthaus 2013, che analizza i "mercati delle competenze" nell'ecosistema del cybercrime.
6. Il ruolo delle tecnologie ICT come motori della "democratizzazione" del crimine è stato evidenziato, in termini generali, da Wall 2007.
7. Si adotta qui il termine *Crime-as-a-Service* (sintetizzato, CaaS), in allineamento con i più recenti report istituzionali di settore (v. EUROPOL 2017; EUROPOL 2023).
8. Per "affiliati" si intendono i soggetti terzi che partecipano attivamente a un *network* di CaaS, contribuendo alla diffusione o esecuzione di attività illecite in cambio di incentivi, come percentuali sui profitti generati. Per "clienti", invece, si intendono coloro che acquistano semplicemente i servizi e/o gli strumenti messi a disposizione, senza entrare a far parte di un programma collaborativo strutturato (come avviene tipicamente nei modelli di *Ransomware-as-a-Service* - RaaS).
9. In tema di RaaS, si rimanda per approfondire, ai recenti studi tecnici di Alwashali–Abd Rahman–Ismail 2021; Karapapas–Pittaras–Fotiou–Polyzos 2020; e Meland–Bayoumy–Sindre 2020.
10. Si rimanderà in tal senso ai recenti report periodici pubblicati da Europol, come il SOCTA (*Serious and Organised Crime Threat Assessment*) e l'IOCTA (*Internet Organised Crime Threat Assessment*), poiché offrono una panoramica aggiornata circa le tendenze del crimine organizzato e delle minacce cibernetiche, inclusi fenomeni come il CaaS; cfr. EUROPOL 2017; EUROPOL 2023.

2.1. Architettura socio-organizzativa

Un primo interrogativo centrale nell'analisi delle fenomenologie criminali riguarda la loro morfologia strutturale. Le evidenze empiriche suggeriscono che il CaaS non corrisponda né a una gerarchia criminale rigida tradizionale né a una rete totalmente decentralizzata, ma che si configuri piuttosto come una struttura, si potrebbe dire, "ibrida". Ossia, da un lato paiono prevalere dinamiche orizzontali, nelle quali attori iper-specializzati (come sviluppatori di *malware*, *broker*, affiliati, amministratori di *marketplace*) cooperano, dall'altro, in alcuni segmenti della catena criminale, sembrano emergere elementi verticali, come figure di coordinamento, intermediari dominanti o leader tecnici, che svolgono un ruolo di supervisione delle attività[11]. Questa natura "ibrida" riflette, in parte, la logica imprenditoriale sottostante al modello CaaS, che, in analogia ai modelli leciti (si pensi al *Software-as-a-Service*), riproduce ecosistemi composti da venditori, fornitori e gestori dotati di ampia autonomia, ma sostenuti da nodi centrali che coordinano o facilitano specifiche operazioni[12]. Pertanto, ne emerge, a livello complessivo, un'organizzazione caratterizzata da: flessibilità (nell'assetto interno), specializzazione professionale, relazioni di durata variabile (alle volte configurate quali collaborazioni "a progetto", in funzione delle esigenze del "mercato") e una forte dipendenza da meccanismi di affidabilità e coordinamento reciproco, più che da una rigida catena di comando, punto su cui si tornerà a breve[13].

Sul versante delle connessioni sociali, uno snodo cruciale del CaaS riguarda il ruolo dei canali di comunicazione attraverso cui gli attori criminali entrano in contatto, si coordinano e costruiscono relazioni di fiducia. I *marketplace* e i forum illeciti (spesso ospitati sul *dark web*, ma presenti anche sulla *surface*[14]) rappresentano i principali spazi in cui i potenziali partecipanti vengono reclutati e in cui vengono ricercate competenze specifiche. In tali ambienti digitali, tuttavia, le preoccupazioni legate all'anonimato generano un senso di incertezza circa la qualità dei beni e dei servizi offerti, rendendo fiducia e reputazione risorse preziose per la cooperazione criminale. Invero, per ridurre il rischio di truffe, prodotti di scarsa qualità o infiltrazioni delle forze dell'ordine, le comunità criminali legate al CaaS fanno ricorso a specifici meccanismi reputazionali[15]. L'accesso ai forum può essere infatti regolato da verifiche preliminari, quote di adesione o sistemi *invite-only*[16] e, in alcuni casi, agli aspiranti membri può venire richiesto di dimostrare le proprie capacità tramite prove

11. Sul punto si veda Patsakis–Arroyo–Casino 2024, per una ampia disamina circa l'iper-specializzazione professionale all'interno delle dinamiche criminali di CaaS.
12. Per approfondire le funzionalità (lecite) del *Software-as-a-Service*, Tsai–Bai–Huang 2014.
13. Per esemplificare, si consideri il modello del *Malware-as-a-Service* (MaaS). La dimensione orizzontale emerge nella presenza di una pluralità di attori iper-specializzati che cooperano tra loro: gli sviluppatori di *malware*, gli *exploit developers*, i *reverse engineers* che forniscono servizi tecnici complementari, mentre gli affiliati, gli *initial access brokers*, i *traffer* e i *phisher* operano come unità incaricate della diffusione e monetizzazione del *malware*. All'interno di questo ecosistema si osservano, tuttavia, anche ruoli verticali che introducono elementi di direzione (o coordinamento). Tra questi, i *core maintainers* (o *lead developers*) definiscono il piano di sviluppo tecnico del *malware* e ne stabiliscono gli standard operativi; gli *infrastructure coordinators* prendono decisioni sull'architettura di comando; i *negotiators* centralizzano le trattative con le vittime (si pensi al RaaS) determinando gli importi dei riscatti; e i *financial controllers* sovraintendono alla gestione dei proventi. Completano il quadro i *recruiters* e i *PR managers*, che contribuiscono alla coesione organizzativa attraverso il reclutamento, la gestione dell'immagine pubblica e il mantenimento della reputazione del "brand" criminale. Per approfondire sul punto, Patsakis–Arroyo–Casino 2024.
14. A questi si affiancano anche canali di comunicazione, come gruppi Telegram e server Discord, utilizzati da individui e gruppi per pubblicizzare i servizi, rivendicare capacità tecniche o vendere prodotti malevoli, cfr. Lykousas–Koutsokostas–Casino–Patsakis 2023.
15. Sul punto, Huang–Siegel–Madnick 2017, che analizzano il CaaS come una vera e propria *supply chain* criminale, individuando nei *criminal marketplace* i principali punti di controllo dell'intero ecosistema.
16. Cfr. Yip–Shadbolt–Webber 2013.

pratiche, come di "hackerare un sito web entro x mesi" per mantenere l'iscrizione[17]. In questo contesto, la reputazione assume il valore di un vero e proprio capitale economico: costituisce la principale forma di "moneta" fiduciaria che abilita la cooperazione tra sconosciuti, influenza la capacità di attirare potenziali affiliati, orienta la fissazione dei prezzi e condiziona l'ingresso nei *marketplace* più ricercati.

Nel complesso, tali caratteristiche socio-organizzative delineano il CaaS come un modello industriale del crimine, fondato su reti associative adattabili, ruoli specializzati e meccanismi reputazionali che fungono da "infrastruttura di fiducia", dando luogo a un ecosistema al tempo stesso stabile (nell'operatività) e volatile (nella capacità di mutare forma), nonché fortemente scalabile sul piano economico.

2.2. Servizi offerti *à la carte*

Come evidenziato sino ad ora, il mercato del CaaS offre una gamma estremamente articolata di servizi, strumenti e competenze, che in letteratura risultano spesso privi di una sistematizzazione comune. In questa sede si propone, a tal fine, di suddividerli in due macrocategorie: i servizi di supporto "diretto", cioè che consentono materialmente di eseguire un attacco informatico o di ottenere un accesso tecnico iniziale al sistema target, e i servizi di supporto "indiretto", comprendenti le attività (ancillari) dirette a sfruttare, monetizzare e/o sostenere l'operazione criminale nel tempo[18]. La prima categoria include tutte le offerte che permettono di condurre un attacco in senso stretto o di stabilire un punto d'ingresso: tra queste rientrano il *botnet-as-a-service*, ovverosia il noleggio di reti di dispositivi compromessi; il *traffic/DDoS-as-a-service*, volto alla generazione di traffico ostile o di attacchi di saturazione (DDoS); il *payload-as-a-service*, che mette a disposizione file malevoli già configurati; l'*exploit-as-a-service*, dedicato alla fornitura o licenza di vulnerabilità; il *bulletproof-as-a-service*, ossia infrastrutture di *hosting* progettate per resistere a *takedown* e investigazioni; e, ancora, le varie forme di *phishing-*, *dropper/delivery-* e *proxy-as-a-service*, incaricate rispettivamente di predisporre campagne di *phishing*, distribuire *malware* attraverso vettori affidabili (o automatizzati) e fornire accessi remoti o instradamenti tramite server compromessi per garantire anonimato ed esecuzione sicura dell'attacco[19].

La seconda categoria, invece, comprende tutte quelle funzioni necessarie per sfruttare economicamente gli attacchi, occultarne le tracce o sostenerne l'operatività. Vi appartengono il *laundering-as-a-service*, che comprende servizi di riciclaggio e il reclutamento di *money mules* per la gestione dei flussi finanziari illeciti; il *marketplace-as-a-service*, che fornisce licenze, infrastrutture e strumenti per la gestione di piattaforme di scambio-offerta criminale; l'*obfuscation-as-a-service* e il *security-checker-as-a-service*, volti rispettivamente a rendere un malware più difficile da rilevare e a verificare la qualità tecnica di un cyberattacco; infine, il *training-as-a-service* e il *recruiting-as-a-service*, che permettono di alimentare l'ecosistema favorendo formazione, specializzazione, ricambio e continuità professionale[20].

I modelli economici maggiormente diffusi tra i venditori paiono essere[21]: (i) le formule in abbonamento, tipiche dei servizi continuativi, che prevedono un pagamento ricorrente in cambio dell'accesso stabile a risorse come *botnet*, servizi di *hosting* o strumenti di offuscamento: si tratta di modelli che garantiscono al fornitore entrate costanti e all'acquirente continuità e aggiornamenti tecnici; (ii) le vendite *one-shot*, che riguardano invece l'acquisto singolo di *tool*, accessi iniziali o *exploit*, spesso senza supporto successivo: sono modalità adatte a prodotti che non richiedono

17. Cfr. Holland 2016, che descrive come forum, *marketplace* e canali di scambio diventino luoghi di "*talent scouting*", nei quali la reputazione tecnica costituisce un asset per attrarre collaboratori affidabili.
18. Per un'analisi longitudinale circa l'evoluzione dell'offerta e della domanda di CaaS all'interno dei forum cybercriminali, si veda Akyazi–van Eeten–Hernández Gañán 2021, che esaminano undici anni di attività su *HackForums*, uno dei più grandi e longevi forum di *cybercrime* in lingua inglese presenti sul *surface web*.
19. *Ibidem*.
20. *Ibidem*, ma si v. anche Huang–Siegel–Madnick 2017.
21. Per approfondire il versante economico-commerciale si rimanda a Huang–Siegel–Madnick 2017.

manutenzione prolungata e che possono essere monetizzati tramite transazioni isolate; (iii) modelli di affiliazione o di *revenue-share*, nei quali l'operatore principale mette a disposizione l'infrastruttura e l'affiliato riceve una percentuale dei profitti, schema particolarmente comune nel RaaS[22].

Si noti ancora come le dinamiche di prezzo e di funzionamento del mercato CaaS risultino fortemente condizionate sia da fattori di offerta (ad esempio i costi di sviluppo, di manutenzione e il livello di rischio percepito dal venditore) sia da fattori di domanda (quali il numero di acquirenti potenziali e il valore dell'obiettivo), ricalcando, ancora una volta, le logiche di business rinvenibili dei mercati leciti. L'evidenza empirica raccolta da Akyazi, van Eeten e Gañán nel 2021[23] relativa a undici anni di dati provenienti da *HackForums*, uno dei principali forum di cybercrime, mostra a tal proposito una diversificazione delle fasce di prezzo e una segmentazione dell'offerta. La parte "bassa" del mercato risulta costituita da servizi automatizzati – come traffico web fraudolento (TRaaS; 7-15 dollari per 1.000 visitatori) o installazioni malware (PLaaS; 0,02-0,1 dollari per installazione) – caratterizzati da un'elevata omogeneità dell'offerta e da margini contenuti, contribuendo alla c.d. democratizzazione dell'accesso al cybercrime. All'estremo opposto si colloca la parte "alta" del mercato, che comprende infrastrutture *zero-day* ed *exploit-as-a-service*, con prezzi che possono superare i 250.000 dollari per licenza o raggiungere 150.000 dollari al mese per pacchetti avanzati. Invece, servizi intermedi, come *botnet-as-a-service* o *bulletproof-as-a-service*, adottano tariffe più contenute, ma regolari (circa 40 dollari/mese per *botnet*, 300 dollari/mese per *hosting*). Nel complesso pare emergere un mercato a doppia velocità: da un lato, servizi a basso costo e facilmente accessibili; dall'altro, un settore altamente specializzato con prezzi elevati e relazioni più stabili, dove reputazione e fiducia fungono da meccanismi di regolazione economica.

3. CaaS e *organized crime* a confronto: convergenze e divergenze

L'analisi condotta nella sezione precedente, indirizzata all'individuazione dei tratti-chiave del CaaS, consente ora di affrontare il passaggio successivo, e conclusivo, dello studio: una comparazione tra il modello CaaS e le principali definizioni criminologiche di criminalità organizzata[24]. Tale confronto permette di interrogarsi se, e in quale misura, gli attori del CaaS possano ricondursi a forme "classiche" di *organized crime*, se il digitale abbia (ri) configurato i tratti-chiave di tali gruppi o se, di conseguenza, emerga l'esigenza di rivedere o integrare le maglie definitorie tradizionali sul tema. Seguendo un approccio metodologico adottato dagli studi criminologici in tema di cybercrime[25], il CaaS può essere messo, in questa sede, in relazione con i quindici elementi costitutivi della criminalità organizzata, tratti dalla letteratura di riferimento[26]. Per ragioni di sistema, tali elementi sono ivi distribuiti in cinque macrocategorie, all'interno delle quali vengono ri-allocati, come segue:

22. Il modello "affiliazione" trova una delle sue espressioni più strutturate nel caso di LockBit, gruppo RaaS tra i più attivi fino al 2024: l'operatore centrale forniva infrastruttura, pannelli di gestione, strumenti di cifratura e supporto tecnico, mentre gli affiliati conducevano gli attacchi *ransomware* e trattenevano una quota significativa dei profitti, secondo un sistema di *revenue sharing* altamente organizzato e supportato da meccanismi reputazionali, cfr. El Emary–Yaghi 2024.
23. Cfr. Akyazi–van Eeten–Hernández Gañán 2021.
24. Sul tema della ri-configurazione delle forme digitali di criminalità organizzata, la letteratura criminologica recente converge sulla necessità di adottare approcci analitici flessibili e non rigidamente dicotomici. Si citi sul punto Picarella 2025, che critica la contrapposizione binaria del "*to be or not to be*" e propone modelli definitori elastici capaci di cogliere la natura ibrida e fluida dei gruppi cybercriminali odierni.
25. L'approccio metodologico richiama quello adottato da Di Nicola–Baratto–Vettori 2025, che ricostruiscono la griglia dei quindici elementi definitori dell'*organized crime*, per poi successivamente applicarli a un corpus di 71 casi giudiziari tratti dal database UNODC SHERLOC, selezionati in quanto caratterizzati da una duplice qualificazione come "cybercrime" e come "partecipazione a un gruppo criminale organizzato".
26. Si rimanda per tale operazione a Varese 2010; Von Lampe 2016.

a) La prima macrocategoria, "strutturale", comprende la presenza di un gruppo composto da almeno tre persone che collaborano stabilmente nella commissione di reati (*group/collaboration*), la durata nel tempo dell'associazione criminale (*duration*), l'esistenza di una catena di comando gerarchica (*hierarchy*) e, più in generale, la presenza di una struttura organizzativa, semplice o complessa che sia (*structure*).
b) La seconda, di natura "economico-funzionale", riguarda l'orientamento primario al profitto economico (*economic profit*), il funzionamento secondo una logica strettamente imprenditoriale (*enterprise*) e l'offerta sistematica di beni o servizi illeciti (*provision of illegal goods/services*).
c) Segue una dimensione "socioculturale", che include l'aspirazione al potere e al controllo sociale o politico (*desire for power*), il radicamento in identità etniche o culturali, spesso territorialmente definite (*ethnicity/subculture*), nonché il ricorso a reti sociali estese e legami relazionali come risorsa operativa (*network*).
d) La quarta categoria concerne aspetti di "governance e coercizione", quali l'impiego di violenza come strumento di gestione interna ed esterna (*corruption/violence*), la ricerca di posizioni monopolistiche in mercati illegali (*monopoly*) e l'esistenza di regole interne e meccanismi di enforcement che disciplinano il comportamento dei membri (*internal regulation and enforcement*).
e) Infine, la quinta macrocategoria, di carattere "operativo", richiama la commissione di reati gravi (*illegal organized activities*) e la capacità del gruppo di generare danni significativi, diretti o indiretti, a individui, istituzioni o sistemi (*harm*).

L'obiettivo della seguente comparazione è, si ribadisce, quello di individuare le aree di invarianza, varianza e assenza rispetto ai modelli tradizionali di *organized crime*, al fine di verificare se e in quale misura l'ambiente digitale agisca come fattore di ri-configurazione adattiva delle dinamiche criminali "organizzate". L'analisi è stata condotta tramite l'elaborazione di un *Network Graph* (Fig. 1), che visualizza per ciascun elemento costitutivo-chiave le tre condizioni analitiche di: invarianza (in verde), varianza (in giallo) e assenza (in grigio) all'interno del modello CaaS, in rapporto alle caratteristiche del crimine organizzato tradizionale.

A seguire i risultati emersi, riportati secondo le cinque macrocategorie sistematiche precedentemente delineate:

a) *Strutturale*: il CaaS presenta alcuni elementi di continuità con la criminalità organizzata tradizionale, in particolare per quanto riguarda la presenza di gruppi composti da più soggetti che cooperano stabilmente e l'esistenza di una struttura organizzativa che, per quanto flessibile, risulta essere riconoscibile (*group, structure*). Invero, nei contesti CaaS è possibile trovare nuclei cooperativi relativamente stabili, reti di affiliati, ruoli differenziati e coordinamento operativo. Tuttavia, altri elementi "classici" – quali la durata nel tempo e la gerarchia (*duration, hierarchy*) – mostrano una varianza. Le organizzazioni CaaS tendono infatti a configurarsi come aggregazioni fluide e a volte temporanee, costituite per il perseguimento di obiettivi specifici (come campagne di attacco, operazioni RaaS) e successivamente disgregate o ri-configurate in funzione delle opportunità di mercato. Ne risulta un assetto che non corrisponde né a una rigida piramide gerarchica né a una rete totalmente dispersa, ma a una configurazione composita (o "ibrida", cfr. par. 2.1). La struttura complessiva alterna così elementi reticolari e momenti di verticalizzazione, riflettendo una adattabilità tipica ai contesti digitali (per loro natura, altamente mutevoli).
b) *Economico-funzionale*: si riscontra una forte invarianza rispetto al modello "classico" dell'impresa criminale. Il CaaS conserva infatti un orientamento esplicito al profitto economico (*economic profit*), adottando logiche di efficienza, scalabilità e mitigazione del rischio tipiche delle organizzazioni imprenditoriali (*enterprise*)[27]. Tale continuità trasla il paradigma dell'impresa criminale in chiave meramente tecnologica: il mercato dei servizi – digitali – illeciti (*provision*) si struttura secondo dinamiche di domanda-offerta, segmentazione,

27. Si v. Schelling 1967, che già proponeva una lettura economica dell'impresa criminale, sostenendo che molte dinamiche di mercato, incentivi e strutturazione organizzativa presenti nelle attività illecite non andavano a differire profondamente da quelle delle imprese legali.

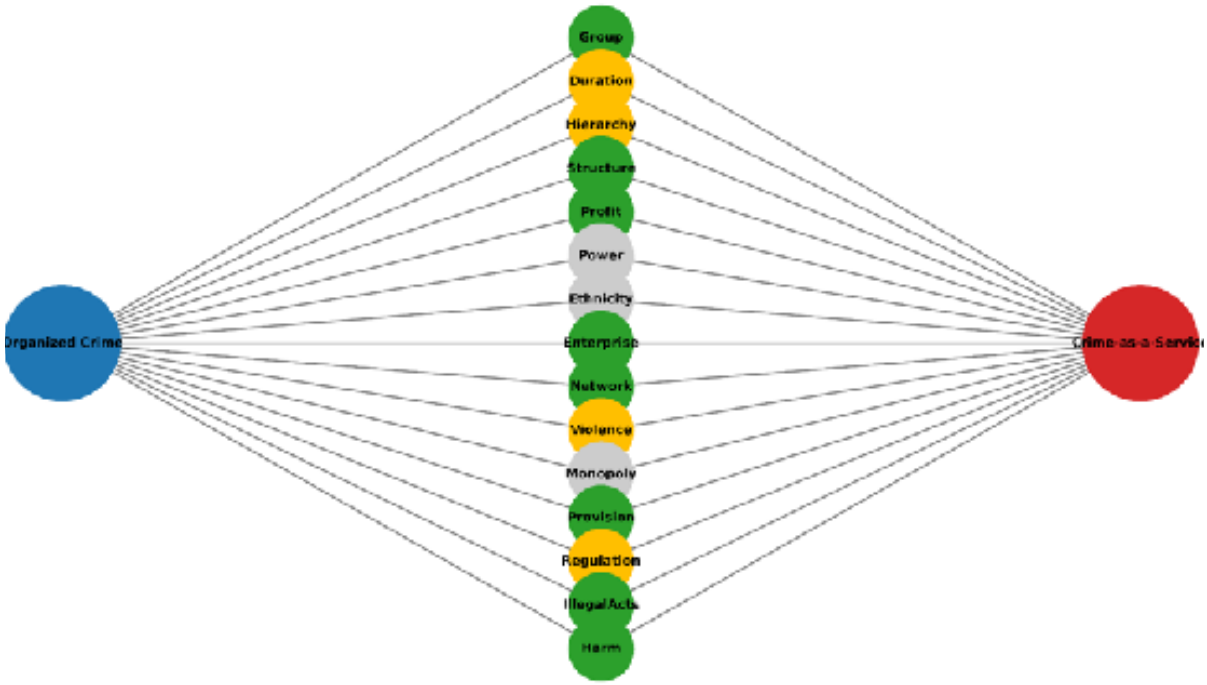

Fig. 1 — *Network Graph elaborato dall'autrice, sui 15 elementi costitutivi dell'organized crime, cfr. Von Lampe 2016 e Varese 2010*

specializzazione funzionale e diversificazione dei prodotti, specularmente a quanto avviene nei mercati leciti.

c) *Socioculturale*: evidenzia i mutamenti più profondi. Nelle reti CaaS, elementi quali il desiderio di potere radicato territorialmente (*power*) e l'appartenenza etnica o subculturale (*ethnicity/subculture*), centrali nei modelli tradizionali di criminalità organizzata, risultano pressoché assenti. Le logiche identitarie e territoriali lasciano infatti il posto a una comunità digitale transnazionale (ma anche, a-territoriale), legata non tanto da vincoli culturali, ma da meccanismi reputazionali e da interessi economici condivisi. La coesione sociale interna (*network*) permane, ma si trasforma: non si fonda più su appartenenze precostituite, bensì su forme di fiducia costruite attraverso i *marketplace* criminali, basate su affidabilità tecnica e capacità di onorare gli impegni. Questa de-territorializzazione determina una vera e propria de-culturalizzazione del legame criminale, in cui il capitale sociale risulta definito dalla reputazione operativa più che dall'identità (o sottocultura) condivisa.

d) *Governance e coercizione*: la governance criminale nel CaaS si esercita attraverso forme di regolazione e coercizione digitali. La violenza, centrale nell'*organized crime* tradizionale (*violence*), viene ricodificata in modalità tecnologiche: si pensi al RaaS, in cui l'estorsione "informatica" sostituisce quella fisica come strumento di intimidazione e pressione sulle vittime. Analogamente, la regolazione interna (*internal regulation and enforcement*) si manifesta tramite programmi di affiliazione online, regole di condotta e sistemi di reputazione condivisi nei *marketplace*, che definiscono in modo vincolante ciò che è consentito e proibito all'interno del gruppo[28]. Quanto al monopolio

28. Si vedano, ad esempio, le *rules of conduct* pubblicate da gruppi RaaS come REvil, LockBit e Conti, che prevedono divieti espliciti (quali di colpire infrastrutture sanitarie o organizzazioni non profit), obblighi operativi (tempistiche di consegna, standard minimi di qualità del *malware*, procedure di negoziazione) e sanzioni in caso di violazione. Tali regole sono spesso integrate da sistemi reputazionali su *marketplace* come *Exploit* o

(*monopoly*), le dinamiche appaiono differenti: il mercato CaaS è infatti aperto, frammentato e altamente competitivo, il che rende improbabile la formazione di posizioni di dominio duraturo o la concentrazione stabile del potere.

e) *Operativa*: Le gravi attività illecite (*illegal activities*) proprie delle reti CaaS, insieme alla loro capacità di ingenerare danni significativi (*harm*), mostrano una sostanziale invarianza rispetto ai modelli tradizionali. Sebbene cambino, digitalmente, gli strumenti e le modalità di esecuzione, il CaaS continua infatti a porre in essere forme di attività criminale coordinate ad alto impatto (si pensi agli attacchi *ransomware* su larga scala), mantenendo un significativo potere lesivo nei confronti di individui, imprese e istituzioni, con impatti sulla sicurezza economica, informativa e, più in generale, sulla stabilità dei sistemi digitali.

4. Prospettive teoriche e giuridiche emergenti

Tirando le fila dell'analisi, il confronto tra il modello CaaS e le definizioni criminologiche di *organized crime* rivela: il passaggio dalle forme di controllo territorializzato a gruppi reticolari e a-spaziali; dalla coercizione fisica a quella tecnologica; dalle gerarchie stabili a strutture "ibride" e fluide. Ne emerge un paradigma in cui il nucleo economico-organizzativo dell'impresa criminale resta pressoché invariato, mentre mutano – digitalizzandosi – i *modi operandi* e le dinamiche relazionali. Tale evidenza richiama la necessità di un'integrazione più stretta tra teoria criminologica e prospettiva giuridico-penale, così da poter inquadrare normativamente la natura organizzata, seppur digitalmente riconfigurata, delle economie del crimine basate sul modello CaaS[29].

In questa direzione, la ricerca criminologica futura dovrebbe approfondire ulteriormente la struttura dei *network* CaaS, le loro dinamiche collaborative e, soprattutto, i meccanismi motivazionali e di affiliazione che guidano la partecipazione degli attori, ancora poco indagati. Comprendere perché e come gli affiliati entrino, permangano o abbandonino tali ecosistemi costituirebbe un passaggio essenziale per formulare strategie preventive realmente efficaci. Parimenti, meriterebbe maggiore attenzione la ricostruzione dei sistemi di regolazione interna e delle modalità di governance criminale, elementi decisivi per spiegare la resilienza di queste reti.

Sul versante normativo, risulta indispensabile una qualificazione giuridica coerente delle forme "organizzate" di CaaS, necessitante di categorie giuridiche flessibili e sensibili alle specificità singole dei modelli *as-a-service*, assieme alla previsione di strumenti investigativi aggiornati – dalla *digital forensics* alle tecniche di *blockchain analytics* – utili per tracciare pagamenti, mappare reti finanziarie e identificare le connessioni operative tra gli attori coinvolti. L'attuale quadro legislativo rimane infatti, in parte, lacunoso (si pensi agli interventi della legge n. 90/2024), e richiederebbe un ripensamento capace di cogliere la natura dei modelli CaaS. In definitiva, una sinergia effettiva tra studi tecnici, criminologia e diritto, fondata su strumenti – teorico/definitori e operativi – adeguati e aggiornati, consentirebbe di comprendere appieno la complessità del CaaS e di elaborare relative strategie di prevenzione e contrasto idonee a fronteggiare tali fenomeni criminali. Il presupposto di fondo di questo studio è il seguente: le definizioni modellano le risposte; e nell'era digitale, solo definizioni capaci di evolvere possono garantire interventi realmente efficaci.

Riferimenti bibliografici

U. Akyazi, M. van Eeten, C. Hernández Gañán (2021), *Measuring Cybercrime-as-a-Service (CaaS) Offerings in a Cybercrime Forum*, in "Proceedings of the Workshop on the Economics of Information Security (WEIS 2021)", 2021

BreachForums, in cui i membri vengono classificati tramite *rating*, *feedback* e *ban list*, strumenti cruciali per garantire affidabilità e disciplina interna. Per approfondire, Hägvall–Valverde 2024.

29. Così anche Whelan–Bright–Martin 2023.

A.A.M.A. Alwashali, N.A. Abd Rahman, N. Ismail (2021), *A Survey of Ransomware-as-a-Service (RaaS) and Methods to Mitigate the Attack*, in "Proceedings of the 14th International Conference on Developments in eSystems Engineering (DeSE 2021)", IEEE, 2021

G.S. Becker (1968), *Crime and Punishment: An Economic Approach*, in "Journal of Political Economy", 1968

M. Castells (1996), *The Rise of the Network Society*, Blackwell, 1996

R. Clarke, D. Cornish (1985), *Rational Choice Theory*, in "Crime and Justice", 1985

D. Cornish, R. Clarke (1986), *The Reasoning Criminal: Rational Choice Perspectives on Offending*, Springer, 1986

A. Di Nicola, G. Baratto, B. Vettori (2025), *Criminological definitions of organized crime on the digital test bench: towards a physical-digital framework*, in "Trends in Organized Crime", 2025

I.M.M. El Emary, K.A. Yaghi (2024), *Machine Learning Classifier Algorithms for Ransomware LockBit Prediction*, in "Journal of Applied Data Sciences", vol. 5, 2024, n. 1

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

EUROPOL (2017), *European Union Serious and Organised Crime Threat Assessment Report (SOCTA) 2017*, in www.europol.europa.eu/, 2017

G. Fiorinelli (2023), *Nomina nuda tenemus? Lo statuto penalistico del crimine informatico tra mutamenti fenomenici e modificazioni semantiche*, in "Discrimen.it", 2023

W. Gibson (1984), *Neuromancer*, Ace Books, 1984

J. Hägvall, G. Valverde, (2024), *A Case Study of DarkDock Marketplace: Seller-Buyer Trust & Reputation in Cybercrime Services*, Linnaeus University, disponibile su DiVA Portal, 2024

R. Holland (2016), *The Hacker Talent Shortage: What Organizations Can Learn from the Recruitment Efforts of Their Attackers*, in "Digital Shadows", 2016

K. Huang, M. Siegel, S. Madnick (2017), *Cybercrime-as-a-Service: Identifying Control Points to Disrupt*, CISL Working Paper n. 2017-17, Massachusetts Institute of Technology, 2017

C. Karapapas, I. Pittaras, N. Fotiou, G.C. Polyzos (2020), *Ransomware-as-a-Service Using Smart Contracts and IPFS*, in "2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)", IEEE, 2020

J. Lusthaus (2013), *How organized is organised cybercrime?*, in "Global Crime", vol. 14, 2013

N. Lykousas, V. Koutsokostas, F. Casino, C. Patsakis (2023), *The Cynicism of Modern Cybercrime: Automating the Analysis of Surface Web Marketplaces*, in "2023 IEEE International Conference on Service-Oriented System Engineering (SOSE)", IEEE, 2023

P.H. Meland, Y.F.F. Bayoumy, G. Sindre (2020), *The Ransomware-as-a-Service economy within the darknet*, in "Computers & Security", vol. 92, 2020

C. Patsakis, D. Arroyo, F. Casino (2024), *The malware as a service ecosystem*, in "Malware: Handbook of Prevention and Detection", Springer Nature, 2024

C. Pecorella (2006), *Il diritto penale dell'informatica*, CEDAM, 2006

L. Picarella (2025), *Criminalità in rete. Dalle piattaforme illegali alle cybermafie*, Donzelli, 2025

L. Picotti (2011), *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, in "Rivista trimestrale di diritto penale dell'economia", 2011, n. 4

T.C. Schelling (1967), *Economics and Criminal Enterprise*, in "The Public Interest", 1967, n. 7

W. Tsai, X. Bai, Y. Huang (2014), *Software-as-a-Service (SaaS): Perspectives and Challenges*, in "Science China Information Sciences", vol. 57, 2014, n. 5

F. Varese (2010), *What is Organized Crime?*, in F. Varese (a cura di), "Organized Crime", Routledge, 2010

K. Von Lampe (2016), *Organized crime: Analyzing illegal activities, criminal structures, and extra-legal governance*, SAGE Publications, 2016

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

D.S. Wall (2007), *The Transformation of Crime in the Information Age*, Polity Press, 2007

C. Whelan, D. Bright, J. Martin (2023) *Reconceptualising organised (cyber)crime: the case of ransomware*, in "Journal of Criminology", vol. 56, 2023, n. 4

M. Yip, N. Shadbolt, C. Webber (2013), *Why forums?: An Empirical Analysis into the Facilitating Factors of Carding Forums*, in "Proceedings of the 5th Annual ACM Web Science Conference", 2013

Sezione monografica

I dati in ambito pubblico tra esercizio della funzione amministrativa e regolazione del mercato

a cura di

Marco Bombardelli, Simone Franca, Anna Simonati

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0261 • articolo non sottoposto a peer review • pubblicato in anteprima il 21 gen. 2026

Marco Bombardelli

Introduzione: il contesto di riferimento per il trattamento dei dati in ambito pubblico

L'Autore è professore ordinario di Diritto amministrativo presso il Dipartimento di Giurisprudenza dell'Università di Trento

Questo contributo fa parte della sezione monografica *I dati in ambito pubblico tra esercizio della funzione amministrativa e regolazione del mercato* a cura di Marco Bombardelli, Simone Franca, Anna Simonati

Nella società moderna il trattamento dei dati personali ha assunto una dimensione nuova sia dal punto di vista quantitativo, sia da quello qualitativo. Sotto il primo profilo, da un lato, gli individui mettono in circolazione quantità sempre maggiori di dati nell'ambito delle proprie relazioni personali e sociali, come pure in quello dei rapporti con le pubbliche amministrazioni. Dall'altro lato, aumentano per numero e dimensioni gli archivi in cui questi dati vengono raccolti e conservati. Sotto il secondo profilo, con la spinta impressa dallo sviluppo delle tecnologie informatiche, questa enorme quantità di dati personali può poi essere analizzata ed elaborata con velocità rapidissima, grazie a sistemi di calcolo molto potenti che ne consentono la correlazione, la combinazione e l'utilizzo per le finalità più disparate. Questo rende sempre più difficile stabilire quali dati possano essere considerati poco rilevanti per la tutela della sfera personale degli individui. Infatti, anche dati apparentemente poco significativi possono diventare importanti nell'ambito di trattamenti che, attraverso la loro combinazione e/o aggregazione con altri dati, consentono di trarre da essi informazioni idonee a condizionare, e talora anche a guidare, i comportamenti dei singoli e l'evoluzione della società.

Questi sviluppi hanno un impatto significativo sul modo con cui il diritto va a disciplinare il fenomeno considerato nella presente sezione monografica. Di esso i principali ordinamenti giuridici hanno cominciato a occuparsi almeno a partire dalla fine dell'Ottocento, in concomitanza con l'accelerazione del progresso economico e tecnologico delle società occidentali. Inizialmente, l'attenzione è stata posta sulle esigenze di riservatezza. Questa viene evidenziata dapprima negli Stati Uniti, secondo l'originale connotazione di *right to be let alone* proposta nel celeberrimo saggio di Warren e Brandeis. Qui la riservatezza è stata configurata come diritto del singolo a evitare intrusioni da parte di altri in una zona intangibile della propria sfera privata, dove vanno salvaguardati, anche nel bilanciamento con la libertà di stampa e di manifestazione del pensiero, i valori di autonomia e dignità propri della persona, in sé e nell'ambito familiare e sociale in cui essa si colloca. In Europa le stesse esigenze sono venute in evidenza a partire dal secondo dopoguerra, con riferimento però soprattutto all'ingerenza dello Stato nella sfera individuale della persona per finalità di controllo, rispetto alla quale si vogliono porre precise barriere a garanzia dei diritti di libertà, particolarmente avvertita dopo l'esperienza dei regimi totalitari che in diversi Paesi europei avevano posto in essere ampie e ripetute violazioni della stessa. La tutela dell'individuo in relazione ai dati personali che lo riguardano viene così originariamente affermata soprattutto con riferimento alla protezione della sua sfera privata, tramite l'imposizione di limiti all'ingerenza nella stessa da parte sia di poteri privati che di poteri pubblici.

Successivamente, però, da un lato, lo sviluppo economico e la sempre maggiore ampiezza dei mercati e delle relazioni tra gli operatori che operano su di essi, dall'altro, l'aumento dell'attività di prestazione degli Stati e la loro conseguente necessità di conoscere i dati personali per soddisfare i propri obblighi positivi verso i cittadini hanno fatto aumentare in modo considerevole l'esigenza di circolazione dei dati personali, riducendo in modo corrispettivo la possibilità di proteggere questi ultimi in termini di libertà negativa. Al contempo, lo sviluppo delle tecnologie dell'informazione e della comunicazione ha fatto crescere in modo esponenziale le potenzialità di utilizzo e trattamento dei dati e con esse le occasioni e le modalità di incidenza non solo nella sfera privata dell'individuo, ma in generale nella sua rappresentazione sociale. Ciò ha condotto a individuare accanto al tradizionale diritto alla riservatezza un più generale diritto alla protezione dei dati personali, che comprende anche la garanzia dell'autodeterminazione informativa. Un diritto, cioè, che oltre a implicare il diritto della persona di negare il consenso alla raccolta e all'uso dei propri dati da parte di altri, comporta anche il diritto della stessa di mantenere un

pieno controllo sui propri dati anche quando per le ragioni più diverse ne ha dovuto dare comunicazione all'esterno. Controllo che implica la possibilità della persona di sapere se qualcuno ha raccolto e sta trattando dati che la riguardano, di conoscere esattamente con quali modalità e per quali finalità i propri dati vengono trattati, nonché di chiedere la rettifica o la cancellazione degli stessi dal trattamento effettuato.

Fino a tempi recenti, comunque, il diritto alla protezione dei dati personali ha continuato a essere considerato principalmente con riferimento alla dimensione individuale. Le preoccupazioni maggiori hanno continuato ad essere rivolte verso la concentrazione di grandi quantità di dati che si viene a creare presso i soggetti che li raccolgono, sempre più grandi e potenti, e la conseguente possibilità di profilazione e di controllo del singolo di cui gli stessi si trovano a disporre. Gli strumenti di tutela sono stati modellati in riferimento ad esse, al fine di consentire agli interessati di sapere che il trattamento esiste, di controllare come viene effettuato ed eventualmente, almeno in alcuni casi, di chiederne l'interruzione. Si è così finora in prevalenza cercato di garantire la tutela dei dati sottoponendo i titolari del trattamento a due obblighi: far sapere che il trattamento esiste e poi riconoscere agli interessati il diritto di accedere ai dati che li riguardano e, nel caso, di chiedere un intervento di modifica del loro trattamento.

Questo approccio alla tutela dei dati personali è quello attualmente prevalente nella normativa nazionale ed europea, che però si trova di fronte a due fenomeni che in parte gli sfuggono e ne richiedono quindi in prospettiva un adeguamento.

Il primo è quello del diffondersi sempre più rapido ed esteso della *big data analytics*, che consente di combinare non solo i dati inerenti alla singola persona, ma anche quelli relativi a grandi gruppi di individui, in base a caratteristiche selezionate come l'età, il genere, il reddito, la professione, la condizione sociale, l'origine etnica e via dicendo, o anche a intere comunità. Oltre che come diritto individuale la tutela dei dati personali richiede così di essere considerata anche come interesse collettivo, da garantire non solo proteggendo il singolo individuo dai rischi di accesso arbitrario ai suoi dati e dalla possibilità di profilazione, ma preoccupandosi anche dei gruppi omogenei di individui e della società nel suo insieme. Si comincia così a considerare l'esigenza di contrastare i rischi che dai trattamenti di dati possono derivare in termini di controllo sociale, di nuove tecniche di sorveglianza, di discriminazione delle minoranze, di condizionamento dell'opinione pubblica e via dicendo.

Il secondo fenomeno è quello del progressivo emergere di una dimensione "patrimoniale" dei dati personali. Sempre più spesso, infatti, la loro cessione ad altri non si configura più soltanto come il presupposto per impostare rapporti di scambio commerciale, ma diventa direttamente l'oggetto di questo scambio, quale corrispettivo che l'utente corrisponde a chi gli fornisce un servizio, soprattutto di natura digitale. Al diritto alla protezione dei dati personali si comincia così a guardare anche secondo una prospettiva diversa, non più solo in termini di diritto fondamentale, ma anche in termini di diritto relativo, inserito in un rapporto di scambio economico, e dunque anche con riferimento agli schemi propri della tutela del consumatore.

È in questo scenario che si collocano le questioni trattate dai diversi contributi raccolti nella presente sezione monografica. Viene preso in esame il ruolo della pubblica amministrazione nel trattamento dei dati personali. Un ruolo che si presenta secondo una duplice connotazione. Da un lato, infatti, l'amministrazione compare come titolare del trattamento dei dati che sono necessari per lo svolgimento delle funzioni che sono ad essa attribuite doverosamente dall'ordinamento per la cura concreta di interessi pubblici. Dall'altro essa assume una dimensione ulteriore, quale soggetto a cui spettano competenze di regolazione, di vigilanza e di controllo dei trattamenti dei dati personali, da chiunque effettuati, finalizzata a garantire la corretta applicazione della normativa in materia. Le due parti della sezione monografica sono dedicate appunto a considerare in modo distinto questi due diversi ruoli, soffermandosi in particolare, per quanto riguarda il secondo, sulla regolazione del mercato.

Per quanto riguarda il ruolo dell'amministrazione come titolare del trattamento, è da osservare come oggi essa sia chiamata a raccogliere, a gestire e a comunicare una quantità di dati molto maggiore che in passato, al trattamento dei quali deve dedicare un'attenzione che un tempo era sconosciuta. Nell'effettuare questo trattamento, le pubbliche amministrazioni devono operare interventi adeguati in materia di protezione dei dati, nei quali va tenuto conto da un lato della natura, dell'ambito di applicazione, del

contesto e delle finalità del trattamento e, dall'altro, del diverso grado di probabilità e di gravità dei rischi che questo può avere per i diritti e le libertà delle persone fisiche. A tal fine esse devono mettere in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato in modo conforme alla disciplina dettata dl GDPR. Ciò richiede interventi molto rilevanti sulla definizione dell'assetto dell'organizzazione amministrativa e anche sulla "proceduralizzazione" di molte attività. Al tempo stesso, però esse devono assicurare lo svolgimento delle funzioni rispetto a cui il trattamento dei dati è strumentale, nell'ambito del quale sono chiamate a raggiungere in modo efficiente ed efficace i risultati di cura degli interessi che a loro sono affidati.

Ciò richiede un adeguato contemperamento tra questa esigenza e quella di tutela dei dati personali, che non deve mai essere presa in considerazione come fine a sé stessa, stando attenti a che gli adempimenti in materia di trattamento dei dati non diventino un ostacolo allo svolgimento della specifica missione affidata all'amministrazione e alla concreta attuazione del principio costituzionale di buon andamento. Non va mai dimenticato, infatti, che l'attività amministrativa è già di per sé sottoposta al principio di legalità, il che consente di individuare con maggiore facilità la base giuridica per il trattamento dei dati personali (v. in tal senso l'art. 2-*ter*, c. 1-*bis*, del d.lgs. 30 giugno 2003, n. 196), del quale comunque deve sempre essere tenuto presente il nesso di strumentalità esistente con il perseguimento delle finalità di interesse pubblico affidate all'amministrazione.

Ma il trattamento dei dati personali nell'ambito delle funzioni svolte dall'amministrazione pone le relative operazioni anche in riferimento ad altri principi dell'attività amministrativa, per l'attuazione dei quali la circolazione dei dati non deve essere impedita, ma al contrario favorita e resa più dinamica. Si tratta in particolare dei principi di trasparenza amministrativa (art.1, legge 7 agosto 1990, n. 241; art. 1, d.lgs. 14 marzo 2013, n. 33) e di comunicazione interna ed esterna fra le amministrazioni pubbliche (art. 2, d.lgs. 30 marzo 2001, n. 165; art 50, d.lgs. 7 marzo 2005, n. 82). Per l'attuazione del principio di trasparenza le amministrazioni sono tenute a comunicare i dati di cui sono in possesso a chi li richiede e, quando si tratta di dati personali, a operare un bilanciamento tra gli interessi di coloro a cui questi dati si riferiscono, la cui tutela diventa particolarmente rilevante in presenza di dati particolari come ad esempio quelli sanitari, e i contrapposti interessi di coloro che invece vogliono conoscerli e che per questo motivo richiedono l'accesso documentale o l'accesso civico. Situazione analoga viene a determinarsi anche quando si considera il modo con cui le pubbliche amministrazioni devono formare, raccogliere, conservare e rendere disponibili e accessibili i propri dati con l'uso delle tecnologie dell'informazione e della comunicazione, che secondo l'art. 50 del d.lgs. n. 82/2005 deve avvenire in modo da consentirne la fruizione e il riutilizzo da parte dei privati e delle altre pubbliche amministrazioni, per queste ultime anche attraverso l'interconnessione e la condivisione delle banche dati. Anche qui l'osservanza della disciplina normativa sulla tutela dei dati personali può introdurre dei limiti a questa possibilità di fruizione, ma certo non può essere intesa come un ostacolo all'attuazione del principio di comunicazione interna ed esterna dei dati stessi.

Risulta quindi evidente che in riferimento all'amministrazione come titolare del trattamento dei dati non si può adottare un approccio all'applicazione delle regole sulla tutela degli stessi che parta dal diniego della possibilità della loro comunicazione: quest'ultima va sempre intesa come prioritaria, anche se le esigenze di tutela dei dati personali possono richiedere adeguate cautele nella sua realizzazione.

Per quanto riguarda invece il ruolo della pubblica amministrazione come autorità di regolazione e di controllo dei trattamenti dei dati personali, da chiunque effettuati, questo pone prima di tutto un'esigenza di definizione delle competenze delle istituzioni chiamate a intervenire. Va tenuta in considerazione la natura trasversale che la raccolta, la gestione e la comunicazione dei dati hanno sulle diverse attività dei soggetti, privati e pubblici, che operano come titolari del trattamento. Questa fa sì che il potere di intervenire sulle modalità con cui i dati vengono trattati dia alle autorità di controllo la possibilità di ingerirsi su un campo di attività molto ampio, strettamente connesso al perseguimento delle finalità imprenditoriali o istituzionali proprie dei titolari. Ciò, da un lato, richiede che l'intervento delle autorità di controllo non si espanda oltre i limiti connessi alle sue competenze specifiche e tenga conto delle ripercussioni che le modalità di trattamento dei dati imposte ai titolari può avere sul perseguimento

delle loro finalità. Dall'altro, quando l'attività nel cui ambito i dati vengono trattati è già di per sé sottoposta a regolazione e controllo da parte di altre amministrazioni, richiede di evitare che la presenza del trattamento dei dati personali nel campo di rilevazione di due diversi sistemi di controllo faccia sorgere interferenze reciproche. Per questo è importante che l'ambito di competenza dell'autorità di controllo sul trattamento dei dati venga coordinato con quello delle altre amministrazioni indipendenti. Occorre che nel loro complesso queste agiscano in modo che i loro interventi risultino coordinati secondo una logica di complementarità, volta ad assicurare la leale collaborazione tra esse e a realizzare nel modo più efficace, al contempo, l'obiettivo della protezione dei dati personali e quello del corretto svolgimento delle attività sottoposte a regolazione pubblica. Questo vale in particolare quando il trattamento dei dati viene a svolgersi nel mercato, nell'ambito di scambi commerciali in cui il trasferimento dei dati non rileva solo in modo accessorio rispetto a transazioni che riguardano altre tipologie di beni e servizi, ma costituisce l'oggetto dello scambio commerciale. In quest'ambito, in relazione all'esigenza di dare protezione ai dati personali sorgono numerosi problemi, legati ad esempio al consenso al trattamento o alle attività di intermediazione dei dati, che risultano particolarmente rilevanti nei mercati digitali. A questi aspetti, in particolare, pongono attenzione gli scritti raccolti nella seconda parte di questa sezione monografica.

Sezione monografica

I dati in ambito pubblico tra esercizio della funzione amministrativa e regolazione del mercato

Parte 1 - Trattamento dei dati e funzione amministrativa

a cura di

Marco Bombardelli, Simone Franca, Anna Simonati

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0242 • articolo sottoposto a peer review • pubblicato in anteprima il 7 nov. 2025

Fabio Francario

Il trattamento dei dati personali per finalità d'interesse pubblico

L'articolo analizza criticamente l'interpretazione e l'applicazione della normativa sulla protezione dei dati personali, con particolare riferimento al trattamento effettuato da pubbliche amministrazioni per finalità di interesse pubblico. Si dimostra come l'interpretazione acritica conduce al risultato di ritenere che l'evoluzione normativa renderebbe il dato personale disponibile per gli operatori economici privati e indisponibile per le pubbliche amministrazioni che agiscono per finalità di interesse pubblico e finisce per tutelare interessi non meritevoli di tutela o illeciti ("paradosso della privacy"). Si sottolinea la illogicità della subordinazione del trattamento per finalità d'interesse pubblico alle stesse condizioni (come il consenso) previste per i privati, in quanto l'azione del soggetto pubblico è già vincolata dai principi di legalità e proporzionalità e soprattutto, a differenza di quella dei privati, deve osservare il principio di trasparenza.

Privacy – Trattamento dati personali – Pubblica amministrazione – Interesse pubblico – Principio trasparenza

The processing of personal data for purposes of public interest

This article critically analyzes the interpretation and application of data protection legislation, with particular reference to data processing by public administrations for purposes of public interest. It demonstrates how uncritical interpretation leads to the belief that regulatory developments would make personal data available to private economic operators and unavailable to public administrations acting for purposes of public interest, thus ultimately protecting interests that are unworthy of protection or are unlawful ("privacy paradox"). It highlights the illogicality of subjecting data processing for purposes of public interest to the same conditions (such as consent) as those for private individuals, as public bodies' actions are already bound by the principles of legality and proportionality and, above all, unlike those of private entities, must observe the principle of transparency.

Privacy – Data protection – Public administration – Public interest – Principle of transparency

L'Autore è professore ordinario di Diritto amministrativo Università degli studi di Siena

Questo contributo fa parte della sezione monografica *I dati in ambito pubblico tra esercizio della funzione amministrativa e regolazione del mercato* a cura di Marco Bombardelli, Simone Franca, Anna Simonati

1. Premessa

È questa è una delle rare occasioni nelle quali il tema del trattamento dati personali viene trattato in ambito accademico da parte della dottrina amministrativistica. L'Associazione Italiana dei Professori di Diritto Amministrativo ha dedicato al tema un incontro infra-annuale nell'aprile del 2022, ma ricordo poi pochissimi altri eventi.

Adesso gli studi iniziano ad avere una certa consistenza anche nella nostra dottrina amministrativistica[1].

Inizialmente sono stati però davvero pochi gli amministrativisti che si sono occupati del tema, che è così rimasto in balìa per lo più di civilisti giuslavoristi e di operatori "tecnici" della materia, che hanno elaborato un nucleo di concetti di base non immediatamente riconducibili alle categorie giuridiche tradizionalmente note e impiegate in ambito civilistico e pubblicistico e che hanno per di più adoperato un linguaggio non solo nuovo, ma spesso ambiguo e contraddittorio. Affrontare il tema significava confrontarsi con un sistema che impiegava linguaggi nuovi, la difficoltà di comprensione dei quali era acuita dalla confusione e contraddittorietà del lemmario impiegato dal legislatore. Basti pensare alla eccessiva leggerezza e scarsa preoccupazione per la coerenza e continuità delle qualificazioni formali dei ruoli e delle funzioni imputate alle figure preesistenti che hanno caratterizzato la declinazione delle figure del "responsabile"[2]. Un nuovo lemmario, il tecnicismo del nuovo linguaggio e l'incertezza e la confusione delle qualificazioni impiegate non hanno certamente incoraggiato l'approccio degli amministrativisti al tema. Sommati ad una oggettiva distrazione intellettuale di fondo sul tema, l'insieme di questi fattori ha fatto sì che, nel momento in cui si sono iniziati a ricostruire gli istituti tipici della materia, sia mancata una lettura anche in chiave "pubblicistica" delle fonti.

Il mancato apporto della dottrina amministrativista in questa prima fase ha condizionato negativamente tanto la interpretazione del GDPR (il Regolamento europeo 2016/679), quanto della normativa nazionale che ha preso corpo nelle diverse scritture e riscritture del nostro Codice della privacy, avvenute sia prima che dopo l'adozione del Regolamento europeo con il d. lgs. 30 giugno 2003 n. 196, il d.lgs. 10 agosto 2018 n. 101 e il d.l. 8 ottobre 2021 n 139. Il mancato apporto della dottrina amministrativistica in questa fase ha cioè impedito di cogliere la specificità delle problematiche tipiche del trattamento dati da parte delle pubbliche amministrazioni, lasciando che l'interpretazione della disciplina del trattamento dati per finalità di pubblico interesse si appiattisse acriticamente sulle stesse regole e principi applicati al trattamento dati operato da soggetti privati e imprese per finalità di lucro o commerciali.

2. La nascita del concetto giuridico di privacy

Intendiamoci. Il concetto di privacy nasce e si sviluppa in ambito privatistico. È un fatto pacifico.

1. Genuessi 2024; Franca 2023; Megale 2023; Ponti 2023; Tigano 2023; Bombardelli 2022; Cardarelli 2021; Cardarelli 2004.
2. Francario 2022; Francario 2021.

Tradizionalmente, la nascita del diritto alla riservatezza viene fatta risalire alla pubblicazione sulla *Harward Law Review* nel 1890 dell'articolo di Samuel Warren e Louis Brandeis *The Right to Privacy*. La storia è nota. Warren aveva sposato la figlia di un noto senatore e la Evening Gazette di Boston pubblicava continuamente indiscrezioni sulla vita matrimoniale di Warren e di sua moglie.

L'articolo avrebbe teorizzato per primo l'esistenza del diritto alla privacy come "the right to let be alone"; il diritto cioè ad essere lasciati soli, non spiati nell'intimità personale. Lo schema teorizzato è quello del diritto assoluto, della persona. Si vuole garantita la inviolabilità dello spazio privato della persona, dello spazio domestico che deve essere protetto da invasioni altrui realizzabili attraverso strumenti mediatici: giornali, foto, video, registrazioni ecc.[3]

Un tale interesse individuale viene ritenuto meritevole di protezione dall'Ordinamento e viene protetto secondo la logica proprietaria propria dei diritti reali o assoluti.

Il diritto, la pretesa, si sostanzia in uno *jus excludendi alios* e l'interesse viene protetto impiegando la tecnica del divieto: il mio spazio non può essere invaso da terzi. Senza il mio consenso.

È indubbio che il tema privacy nasce quindi come questione tipicamente di diritto privato, di tutela di un interesse esclusivamente privato, individuale, alla riservatezza della propria vita privata e dei luoghi e spazi in cui essa si esplica.

Ma si tratta di una protezione che, per così dire, nasce e muore nell'ambito del diritto privato, senza assumere una speciale o specifica rilevanza se ci si sposta nell'ambito pubblicistico e si viene a contatto con l'azione dei pubblici poteri finalizzata alla cura dell'interesse pubblico, che, come si sa, per quel che riguarda la creazione, modificazione o estinzione dei rapporti giuridici è governata da principi diversi da quelli del consenso e della disponibilità delle situazioni giuridiche soggettive .

Si può anzi dire che, in ambito pubblicistico, avvenga esattamente il contrario. Nel senso che, se la soddisfazione di un interesse personale di un privato cittadino è subordinata alla prestazione di un'attività amministrativa ovvero se ragioni di pubblico interesse rendono il privato destinatario di un'attività amministrativa, l'interesse ritenuto meritevole di protezione dall'Ordinamento non è certamente quello (privato, individuale) alla riservatezza, ma quello pubblico alla trasparenza e conoscibilità dell'attività amministrativa che viene posta in essere[4].

A ben vedere, ciò avviene per una ragione molto semplice, perché, se si è destinatari di provvedimenti o decisioni (rese d'ufficio o a domande di parte) con cui si esercitano pubbliche funzioni, l'identità dei soggetti destinatari deve essere nota. Quando sono in gioco l'interesse pubblico e l'impiego di risorse della collettività, il principio democratico impone di conoscere *perchè* si fa una cosa e *chi* ne è beneficiario o danneggiato[5].

È chiaro quindi che, finchè si parla di privacy, nella primigenia accezione, la protezione dell'interesse non travalica l'ambito privatistico perchè il confine con il diritto pubblico è molto chiaro e netto. Si tratta di un confine tracciato dal passaggio dal principio della disponibilità degli interessi privati a quello della trasparenza dell'azione amministrativa finalizzata alla cura del pubblico interesse. Per esemplificare, questo significa che, finchè rimango nel mio spazio domestico, l'interesse è ritenuto meritevole di protezione. Verso chiunque. Pubblica amministrazione compresa. Ma, se "esco di casa", per chiedere qualcosa alla pubblica amministrazione o per usare beni pubblici (*non miei*), i rapporti giuridici che si creano e vivono attorno alla persona sono governati dal diritto pubblico e non da quello privato. E lo stesso è a dirsi se la Pubblica Amministrazione *entra* nella mia sfera personale perché c'è una norma di legge che attribuisce a tali Autorità questo potere. Così come può avvenire e avviene per qualsiasi altro diritto, che può essere "sacrificato" nel rispetto del principio di legalità e dei principi fondamentali dell'azione amministrativa che condizionano l'esercizio del potere in ragione del fine pubblico perseguito e della proporzionalità rispetto al risultato[6].

3. Rodotà 2007.
4. Per tutti Corrado 2023 e ivi ulteriori riferimenti a dottrina e giurisprudenza.
5. Per tutti Romano Tassone 1996 (ripubbl. 2024); Romano Tassone 1987.
6. Per tutti Corso 2023 e ivi ulteriori riferimenti a dottrina e giurisprudenza.

3. L'evoluzione del concetto: da privacy a trattamento dei dati personali. Il GDPR e la normativa nazionale

Nel diritto contemporaneo il concetto di privacy si è però evoluto ed ha assunto la forma della protezione dei dati personali. Non si tratta di una mera variazione lessicale. Alla diversità del significante si ricollega anche una diversità di significato.

Il concetto non è più lo stesso, non è identico. Anzi. Sembra profondamente mutato.

La tutela sembra infatti assumere come oggetto una vera e propria identità digitale: l'interesse regolato non è più solo quello al controllo della diffusione di notizie o immagini sulla persona, ma al controllo di tutte le informazioni che consentono di identificare la persona fisica (nascita, età, codice fiscale, ecc.). La nozione poi si allarga e ricomprende qualsiasi uso del dato personale. "Trattamento" è non solo la pubblicazione, ma anche l'acquisizione del dato, la sua raccolta e conservazione, il suo trasferimento o messa a disposizione di soggetti terzi.

Tutto questo ha come conseguenza che i dati personali divengono oggetto di un bene giuridico autonomo, diverso dallo spazio privato personale che deve essere protetto da invasioni altrui, che diventa così soggetto alle comuni regole sulla circolazione dei beni giuridici. Si discute se sia ancora valido o meno un paradigma proprietario o se il bene vada diversamente qualificato[7], ma è indubbia l'autonomia assunta sul piano oggettivo dal bene – dato personale.

L'interrogativo che a questo punto è giusto che un amministrativista si ponga è se e quali conseguenze questa evoluzione abbia avuto nell'ambito del diritto pubblico, nei confronti delle pubbliche amministrazioni.

Nella originaria versione del d.lgs. 30 giugno 2003 n. 196, il nostro Codice della privacy dettava disposizioni specifiche per i trattamenti in ambito pubblico nella Parte seconda (artt. 46 ss.), precisando, nella Parte prima dedicata ai principi generali, che "qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali" (art. 18) e che "Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito, fermo restando quanto previsto dall'art. 18, c. 2, anche in mancanza di una norma di legge o regolamento che lo preveda espressamente" (art. 19). Nessun divieto generalizzato per il trattamento dei dati personali comuni o ordinari e possibilità pacifica che, ove si renda necessario per esigenze di cura del pubblico interesse, il diritto alla protezione dei dati personali possa essere limitato o condizionato senza che ciò debba essere espressamente previsto da una norma di legge[8].

Com'è noto, nell'aprile del 2016 viene adottato il c.d. GDPR, ovvero il Regolamento del Parlamento europeo e del Consiglio n. 2016/679, che, sarebbe sempre bene ricordare, viene adottato per "rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione" quando vi sia "connessione con un'attività commerciale o professionale". Così come sarebbe sempre bene ricordare che, in linea di principio, il Regolamento vieta in realtà il trattamento solo di particolari categorie di dati personali ("dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché ... dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona" – art. 9), prevedendo che il divieto non si applichi se "l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche" ovvero se "il trattamento è necessario per motivi di interesse pubblico"; e che, per il trattamento dei dati ordinari, è comunque sempre richiesta come condizione di liceità l'esistenza di un consenso espresso al trattamento, ovvero la necessità di adempiere ad un obbligo legale o la necessità "per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento", chiaramente considerate come condizioni di liceità distinte e tra loro alternative (art. 6). Nel sistema disegnato dal GDPR[9], la necessità per motivi d'interesse pubblico rappresenta quindi una base giuridica del

7. Per tutti Castaldo 2024 ed ivi ulteriori riferimenti.
8. Sulla disciplina così come originariamente recata dal d.lgs. 30 giugno 2003 n. 196 per tutti Cirillo 2004.
9. Finocchiaro 2017; per la visione d'insieme del quadro disegnato dal GDPR per tutti Pizzetti 2016.

trattamento, distinta e alternativa tanto alla espressa previsione legale della necessità del trattamento, quanto alla prestazione del consenso da parte dell'interessato. Istituzionalmente, una tale valutazione è rimessa alla pubblica amministrazione e l'autonomia rispetto alle altre possibili basi giuridiche del trattamento è rimarcata anche dalla disciplina di istituto assolutamente centrale nel sistema disegnato dal GDPR, ossia il diritto all'oblio, nel momento in cui l'art 17 precisa che il diritto dell'interessato, di ottenere dal titolare del trattamento la cancellazione dei dati personali quando questi "non sono più necessari rispetto alle finalità per le quali sono stati raccolti o trattati", non sussiste nei casi in cui il trattamento sia necessario "per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento". Chiara conferma che la valutazione di stretta necessarietà del trattamento rispetto al fine perseguito è sottratta alla disponibilità dello stesso interessato ove effettuata dalla pubblica amministrazione nell'esercizio di pubblici poteri o per l'esecuzione di un compito svolto nel pubblico interesse.

In attuazione del Regolamento, il nostro Codice subisce rilevanti modifiche, che concorrono a originare le incertezze interpretative cui si è già fatto cenno.

Il d. lgs. 101/2018 abroga quasi tutte le disposizioni specificamente dettate per i trattamenti in ambito pubblico nella Parte seconda del Codice (con la significativa eccezione, però, tra le altre, di quelle relative ai dati giudiziari) e introduce l'art. 2-*ter* (base giuridica per il trattamento dei dati personali effettuato per l'esecuzione di un compito d'interesse pubblico e connesso all'esercizio dei pubblici poteri) che precisa che "la base giuridica è costituita esclusivamente da una norma di legge o nei casi previsti dalla legge di regolamento" [10]. Successivamente, a seguito dell'esperienza che matura nel contesto della pandemia Covid, il d.l. 139/2021, convertito con modificazioni dalla l. 205/2021, interviene espressamente per modificare il citato art. 2-*ter* del Codice novellato eliminando dalla formulazione normativa del primo comma l'avverbio "esclusivamente" e l'espressione "nei casi previsti dalla legge", al fine appunto di precisare che "la base giuridica prevista dall'art 6 par. 3 lett b) del regolamento è costituita da una norma di legge o di regolamento o da atti amministrativi generali". Oltre ad altre significative modifiche, introduce poi il comma 1-*bis* al fine di precisare che per le amministrazioni pubbliche e soggetti equiparati il trattamento dei dati personali "è anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri a essa attribuiti"[11].

4. Il punto critico

Dov'è il punto critico, di particolare interesse per l'amministrativista, di un siffatto quadro normativo?

È nell'incertezza sulla necessità o meno, in assenza dell'esplicito consenso dell'interessato, di una espressa previsione di legge affinchè una pubblica amministrazione possa trattare dati per finalità d'interesse pubblico. O, se si preferisce, della distinzione e dell'autonomia della fattispecie della necessità per motivi d'interesse pubblico (che suppone una valutazione amministrativa della necessità del trattamento) rispetto all'ipotesi della necessità di adempiere un obbligo legale (che suppone un'attività vincolata).

L'interpretazione più restrittiva, volta a consentire il trattamento solo in presenza di una norma espressamente attributiva di tale potere, sottraendo all'amministrazione la valutazione della sua necessità per finalità di pubblico interesse, ha ispirato e orientato la prassi dell'Autorità garante nazionale.

Prima ancora d'interrogarsi sulla correttezza sotto il profilo metodologico, vale la pena sottolineare quali siano i risultati ai quali conduce una siffatta interpretazione.

Anche solo un breve campionario è in grado di dimostrare che sottrarre all'Amministrazione la valutazione della necessarietà del trattamento per assicurare la cura dell'interesse pubblico diventa un fattore di paralisi dell'azione amministrativa e uno strumento di tutela di interessi che l'Ordinamento in realtà non ritiene affatto meritevoli di tutela. Anzi, che il più delle volte considera illeciti.

Mi limito a soli tre esempi.

È noto il contrasto insorto durante il periodo pandemico tra l'Autorità garante e le amministrazioni

10. Modafferri 2021; in generale sulla novella del Codice per tutti Pizzetti 2021.

11. Per approfondimenti Francario 2021.

impegnate a contrastare l'emergenza pandemica con misure di prevenzione sanitaria e di sostegno dell'economia. Esemplare in tale contesto è il caso della sanzione comminata all'INPS per aver effettuato verifiche e controlli sulla effettiva spettanza del diritto al cd bonus Covid in capo ai percettori. L'erogazione delle misure indennitarie previste per sostenere le categorie di lavoratori e professionisti colpite dalle misure del *lockdown* è subordinata alla condizione che i destinatari non fossero già titolari di pensione o iscritti ad altra forma previdenziale obbligatoria o titolari di un rapporto di lavoro dipendente, status che i beneficiari devono limitarsi ad autodichiarare. L'INPS avvia le verifiche incrociando i dati fiscali dei richiedenti con quelli ricavabili dai siti pubblici delle camere e degli enti territoriali e locali per accertare se fossero stati indebitamente percepiti anche da parlamentari o amministratori pubblici, come ampiamente riportato dagli organi di stampa e dai media, ma viene multata per ben 300.000 euro perché, a detta del Garante, avrebbe compiuto attività non indispensabili o non necessarie per lo svolgimento della funzione di vigilanza e per aver agito senza avere preventivamente calcolato i rischi che il trattamento dati presentava per i diritti e le libertà degli interessati. L'INPS viene multata e arresta il procedimento di verifica, evitando così di accertare se vi fossero state indebite percezioni di contributi Covid. Gli indebiti percettori rimangono ignoti[12].

Al di fuori del contesto pandemico, altra situazione largamente diffusa e immediatamente rappresentativa delle conseguenze negative dell'interpretazione restrittiva è quella che si riscontra nell'impiego dei sistemi di video sorveglianza da parte degli enti locali nell'accertamento degli illeciti amministrativi previsti dalla normativa in materia ambientale, con specifico riferimento alla violazione del divieto di abbandono o deposito di rifiuti sul suolo. Anche qui esiste una casistica davvero ampia di provvedimenti dell'Autorità garante che sanzionano le amministrazioni locali, ree di aver collocato sistemi di video sorveglianza sulle strade pubbliche senza averne dato "adeguata" informazione[13]. Si badi: non perché non sia stata data alcuna pubblicità, ma perché si ritiene insufficiente quella comunque esistente. L'applicazione della normativa sulla protezione dei dati personali finisce con il proteggere l'interesse, in realtà nient'affatto meritevole di tutela, dei contravventori.

Il terzo esempio che mi limito a fare questa volta non è immediatamente riconducibile a un'attività del Garante, ma è parimenti frutto dell'interpretazione restrittiva delle norme che consentirebbero il trattamento dati per finalità d'interesse pubblico e dà l'idea del livello di diffusione che tale interpretazione ha inspiegabilmente avuto nella prassi. Mi riferisco alla questione dell'oscuramento dei dati personali nei provvedimenti giudiziari.

Con il chiaro intento di impedire la possibilità di risalire anche indirettamente al caso concreto deciso, anche quando non si è in presenza di quei dati personali particolari o sensibili protetti da un divieto di divulgazione o quando l'oscuramento non sia stato chiesto nemmeno dal diretto interessato, le sentenze spesso e volentieri vengono pubblicate nelle banche dati istituzionali omettendo sempre e comunque nominativo e generalità delle persone fisiche. Non solo. L'omissione si estende spesso al nome delle persone giuridiche, ovvero colpisce indiscriminatamente tutte le parti del giudizio. Diffusa e crescente è anche la prassi di omissare, nei giudizi d'impugnazione, persino la data e gli estremi dei provvedimenti del giudizio di primo grado o, più in generale, degli stessi provvedimenti giurisdizionali citati come precedenti. In alcuni casi finanche del tribunale adito. In altri ancora vengono omissati data ed estremi del provvedimento impugnato o delle stesse autorità pubbliche emananti.

Com'è possibile che si arrivi al punto di nascondere i dati identificativi non solo delle persone fisiche, ma anche delle persone giuridiche e persino delle stesse pronunce giurisdizionali e delle autorità giudicanti?

Se si è arrivati a questo punto, è evidente che c'è qualche grave distorsione al fondo del sistema sulla quale occorre riflettere.

La situazione è stata denunciata dall'Associazione Italiana dei Professori di Diritto Amministrativo in un apposito appello che ha cercato di richiamare l'attenzione sul grave pregiudizio che viene in tal modo arrecato alla possibilità di controllo democratico da parte della società civile su una delle

12. Per approfondimenti si rinvia a Francario 2023.

13. Genuessi 2024.

forme fondamentali di esercizio della sovranità popolare e sul fatto che in tal modo le decisioni giurisdizionali diventano non intellegibili, anche da parte di chi sia provvisto della particolare preparazione culturale e giuridica che potrebbe essere richiesta dalla eventuale complessità della decisione, perché se ne nasconde volutamente il contenuto proprio per evitare che si possa mai individuare il caso al quale si riferisce.

L'interpretazione restrittiva delle norme che regolano il trattamento dei dati personali per finalità di pubblico interesse, completamente appiattita, senza distinzioni, su quella propria dei rapporti inter privati, è già di per sé difficilmente spiegabile per il trattamento per finalità di pubblico interesse generalmente considerato, ma nel caso delle pronunce giurisdizionali viene veramente superato ogni limite. L'interpretazione non è più soltanto opinabile sul piano valoriale, ma è chiaramente *contra legem*.

Lasciamo anche un attimo da parte il fatto che il GDPR (art. 6) prevede che il trattamento è lecito se "necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" o quando è "connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" e che basterebbe pertanto osservare che le sentenze sono espressione di una funzione sovrana e che l'obbligo di pubblicazione deriva da norma di legge. L'osservazione rimane comune a tutti i casi di trattamento per finalità di pubblico interesse.

Il fatto veramente sconcertante è che, nel caso dei provvedimenti giurisdizionali, le norme specificamente dettate dal Codice nazionale (le uniche che, come ricordato, sono rimaste sempre ferme anche quando le altre norme del d.lgs. 30 giugno 2003 n. 196 che disciplinavano il trattamento dei dati per finalità di pubblico interesse erano state abrogate dal d.lgs. 101/2018) hanno sempre espressamente previsto che "le sentenze e le altre decisioni dell'autorità giudiziaria di ogni ordine e grado depositate in cancelleria o segreteria sono rese accessibili anche attraverso il sistema informativo e il sito istituzionale della medesima autorità nella rete Internet osservando le cautele previste dal presente capo" (art. 51, co. 2); che i dati identificati degli interessati riportati sulla sentenza o provvedimento possono essere omissati su richiesta di parte, che spetta però all'autorità giudiziaria accogliere o disporre anche d'ufficio se fondata su "motivi legittimi" o per tutelare la "dignità degli interessati" (art 52, co. 1 e 2); che l'omissione di "generalità, dati identificativi o altri dati anche relativi a terzi dai quali può desumersi anche indirettamente l'identità di minori, oppure delle parti nei procedimenti" è doverosa soltanto se si tratti di "persone offese da atti di violenza sessuale" o se si verta "in materia di rapporti di famiglia e di stato delle persone" (art. 52 co. 5)[14]. "Fuori dei casi indicati nel presente articolo", conclude il comma settimo dell'art. 52 del Codice, "è ammessa la diffusione in ogni forma del contenuto anche integrale di sentenze e di altri provvedimenti giurisdizionali".

5. L'interpretazione giurisprudenziale

L'interpretazione restrittiva, diffusa nella prassi, delle norme che disciplinano il trattamento dati per finalità di pubblico interesse disegna un quadro poco incoraggiante: l'applicazione della normativa sul trattamento dei dati personali finisce troppo spesso con il tutelare interessi che sul piano sostanziale l'Ordinamento non ritiene affatto meritevoli di tutela, ma che, al contrario, qualifica illeciti (l'indebito percettore di sussidi pubblici; l'autore di illeciti ambientali) o riduce l'esercizio della funzione giurisdizionale ad un fatto privato, riservato ai soli diretti interessati, che nessun altro *cives* avrebbe diritto di conoscere.

Sembra però possibile intravedere un po' di luce in fondo a questo tunnel, che lascerebbe indurre a un certo ottimismo.

Lo spiraglio di luce, che sembrerebbe schiudersi sempre più, è dato dal fatto che, quando i provvedimenti del Garante o le questioni vengono

14. Che la scelta nel senso di una sostanziale e massiva anonimizzazione sarebbe "eccessiva rispetto non solo al confliggente diritto all'informazione ma anche alle stesse esigenze di privacy come delineate dal GDPR" è del resto sottolineato anche nelle conclusioni della relazione del Servizio Studi della Corte Costituzionale a cura di Patatini–Troncone 2020; analoghe le conclusioni dello studio compiuto dall'Ufficio del Massimario della Corte Suprema di Cassazione a cura di Calvarese–Giusti 2005, nelle quali si sottolinea che l'anonimizzazione può avvenire solo nei casi in cui è espressamente prevista da una norma di legge o, su richiesta dell'interessato, solo previo bilanciamento da parte del giudice dei contrapposti interessi in gioco.

portate all'attenzione dell'autorità giudiziaria, l'accertamento giurisdizionale sembra ripristinare la corretta interpretazione delle norme sul trattamento dati per finalità di pubblico interesse. Proprio in materia di oscuramento dei dati personali nei provvedimenti giurisdizionali merita di essere segnalata una recente sentenza del TAR Lazio, Sez. Prima, 17 aprile 2025 n. 7625, che ben chiarisce i termini della corretta interpretazione della normativa in materia di trattamento dati personali. Nel perseguimento degli obiettivi di digitalizzazione PNRR, il Ministero della Giustizia riorganizza l'archivio giurisprudenziale nazionale (a.g.n.) sdoppiando la banca dati esistente e creando due distinte: una prima, riservata ai magistrati; una seconda, pubblica, accessibile a chiunque previa autenticazione digitale (SPID, CIE etc). Sentenze e provvedimenti inseriti nella seconda vengono anonimizzati, oscurando nomi delle parti e date. Alcuni professori e avvocati, anche in qualità di curatori di una nota rivista dedita alla pubblicazione delle più rilevanti decisioni dei tribunali delle imprese o attinenti al diritto commerciale (*Giurisprudenza delle imprese*), ricorrono al TAR lamentando che la massiva anonimizzazione (nella banca dati pubblica) dei nomi delle parti (persone fisiche e giuridiche) e delle date (ivi comprese quelle del provvedimento, ovvero quelle delle sentenze citate) rende inutile l'uso della banca dati pubblica perché rende impossibile lo studio dell'atto, precludendo il perseguimento dei fini stessi per i quali è nata la rivista. La sentenza accoglie il ricorso affermando senza mezzi termini "di non poter considerare ragionevole, proporzionata o necessaria la decisione di anonimizzare tutti i provvedimenti pubblicati nella banca dati pubblica. Invero, se l'obiettivo è garantire la diffusione della cultura giuridica, rendendo conoscibili gli indirizzi ermeneutici giurisprudenziali che, sebbene non vincolanti, possono guidare l'azione degli operatori giuridici, risulta chiaro che oscurare totalmente le informazioni circa alcuni dati di fatto rende, sostanzialmente, impossibile (o comunque assai complesso) comprendere l'esatta portata del pronunciamento".

Dopo aver sottolineato *che* "la disciplina positiva prevede, in linea generale, la pubblicazione delle pronunce rendendole accessibili a tutti mediante un sistema informativo istituzionale", *che* "la diffusione (ivi compresa quindi anche la pubblicazione in una banca dati accessibile alla generalità dei cittadini) debba avvenire con oscuramento dei dati personali solamente in alcune limitate ipotesi, ossia su richiesta della parte interessata (art. 52, comma 1 d.lgs. 196/2003), oppure d'ufficio allorquando ciò risulti necessario per tutelare i diritti e la dignità dell'interessato (secondo comma)", *che* "salvo il caso peculiare dei procedimenti coinvolgenti rapporti di famiglia, di stato delle persone ovvero minorenni (quinto comma), ove è direttamente la legge a vietare la diffusione dei dati personali le fattispecie regolate dall'art. 52, commi 1 e 2 d.lgs. 196/2003 rimettono all'autorità giudiziaria procedente la decisione sull'oscuramento o meno dei dati personali" e *che* "in assenza di determinazione del giudice, la legge ammette espressamente la diffusione del contenuto integrale delle pronunce giurisdizionali (v. art. 51, comma 2 e art. 52, comma 7 d.lgs. 196/2003)", la sentenza afferma chiaramente *che* "il principio di pubblicità espresso dall'art. 6 Cedu (e implicitamente dall'art. 111 Cost.) si debba estendere oltre l'istante della celebrazione dell'udienza, involvendo anche (e soprattutto) l'esito del processo, ossia la sentenza, la quale deve essere di regola resa disponibile in maniera integrale al pubblico. Ad analoghe conclusioni conduce una lettura teleologicamente orientata anche dell'art. 47 della Carta dei diritti fondamentali dell'Unione europea (Carta di Nizza)". Conclude quindi affermando *che* "va ritenuta contraria al disposto degli artt. 51 e 52 d.lgs. 196/2003 la decisione dell'amministrazione della giustizia di oscurare in maniera generalizzata i dati personali delle parti coinvolti in tutti i procedimenti civili pubblicati nella b.d.p.".

Si può segnalare al riguardo come la pronuncia si muova tutto sommato nel solco tracciato dalla sentenza CGUE, Prima Sezione, 24 marzo 2022 causa C – 245/20 (*Rechtbank Midden – Nederland*), la quale ha escluso la possibilità di un sindacato da parte dell'Autorità garante nazionale sul trattamento dei dati personali fatto da parte dall'autorità giudiziaria affermando chiaramente "che il fatto che un organo giurisdizionale metta temporaneamente a disposizione dei giornalisti documenti di un procedimento giurisdizionale, contenenti dati personali, al fine di consentire loro di riferire in modo più completo sullo svolgimento di tale procedimento rientra nell'esercizio, da parte di tale organo giurisdizionale, delle sue 'funzioni giurisdizionali', ai sensi di tale disposizione".

Altro spiraglio di luce. Ho detto in precedenza del caso INPS. Anche in tal caso possiamo constatare che, proposto ricorso avverso la multa irrogata dal Garante, il ricorso viene integralmente accolto dal Tribunale di Roma, XVIII Sez. Civile (sent. 24 marzo 2022). *Inter alia*, la sentenza afferma espressamente che il rischio di veder revocata l'erogazione di un beneficio cui non si è avuto diritto non è meritevole di considerazione giuridica e che l'aspettativa del beneficiario di un sussidio di un successivo controllo in merito alla effettiva sussistenza delle condizioni richieste deve ritenersi assolutamente ragionevole. Sempre per rimanere alle condotte censurate dal Garante nel periodo pandemico, si può citare anche un'altra interessante pronuncia resa questa volta dal Tribunale di Udine il 20 novembre 2023 che annulla la sanzione irrogata a Insiel spa, società in house della Regione Friuli Venezia Giulia, per aver elaborato, dai dati raccolti nei fascicoli sanitari elettronici e messi a disposizioni dai medici di medicina generale, elenchi delle persone particolarmente fragili per assicurare una più efficace prevenzione e pianificazione della vaccinazione nel contesto pandemico, condotta che il Garante aveva censurato come illecita ritenendola priva di una idonea, specifica base giuridica, priva del consenso degli interessati e non necessaria.

6. Conclusioni

Le pronunce citate sono espressione di un orientamento che è auspicabile venga a crescere e consolidarsi sempre più per evitare quello che altrimenti potrebbe esser definito come un vero e proprio paradosso della privacy, che si avrebbe se l'interpretazione porta a rovesciare l'originario bilanciamento tra interesse pubblico e privato, tra sfera pubblica e privata, rendendo disponibile il bene-privacy per imprese e operatori economici, e indisponibile per la pubblica amministrazione quando deve operare nel pubblico interesse.

Il rischio che si corre applicando la normativa in tema di protezione dei dati personali in una maniera acritica, accomunando il regime del trattamento per finalità di pubblico interesse a quello proprio dell'uso commerciale tra privati, è proprio quello di rendere disponibile il diritto da parte di soggetti privati e imprese, che vengono autorizzati all'uso economico dei dati personali in base ad un consenso che risulta prestato secondo formule di rito standardizzate e non negoziabili, e a rendere per converso indisponibile in ambito pubblico anche il trattamento dei dati comuni e ordinari.

Se l'evoluzione della privacy da "right to let be alone" a diritto al trattamento dei dati personali è servita, per un verso, nel campo del diritto privato, a patrimonializzare il diritto di riservatezza per consentirne l'uso dei big data previo consenso (specifico) dell'interessato; e se, per l'altro, è servita ad oscurare regole e principi di trasparenza e conoscibilità dell'azione dei pubblici poteri, il risultato appare francamente inaccettabile.

Nell'interpretazione non può non assumere rilevanza il fatto che il soggetto pubblico è già di per sé tenuto ad agire secondo finalità predeterminate dalla legge e nel rispetto del principio di proporzionalità, mentre il privato no. E che è quindi logico subordinare la possibilità di trattare il dato personale al previo consenso del soggetto interessato e di limitare il trattamento al fine per il quale il consenso è stato prestato ai soli casi in cui la base giuridica del trattamento è data appunto dal consenso, e non anche nei casi in cui la base giuridica è nelle necessità per finalità di pubblico interesse.

Se non si muove da questa considerazione, si arriva a un risultato assolutamente inaccettabile in termini valoriali; perchè significherebbe appunto che l'evoluzione della disciplina (e del bene tutelato), dalla privacy-riservatezza al trattamento dei dati personali, avrebbe avuto unicamente l'effetto di dare un prezzo al diritto alla riservatezza e di renderlo così disponibile per gli usi commerciali del mercato digitale globale della società moderna; e di renderlo per contro indisponibile proprio laddove i rapporti giuridici devono essere invece istituzionalmente regolati sulla base di un principio di trasparenza e non di riservatezza. Laddove cioè il trattamento è necessario per finalità di pubblico interesse o per l'esercizio di funzioni pubbliche.

Riferimenti bibliografici

M. Bombardelli (2022), *Dati personali (trattamento dei)*, in "Enciclopedia del Diritto: i tematici, 3. Funzioni amministrative", Giuffrè, 2022

E. Calvarese, A. Giusti (a cura di) (2005), *Corte di Cassazione e tutela della privacy: "l'oscuramento" dei dati identificativi nelle sentenze*, Corte di Cassazione, Ufficio del Massimario, 5 luglio 2005

F. Cardarelli (2021), *Base giuridica per il trattamento dei dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in G. Finocchiaro, R. D'Orazio, O. Pollicino, G. Resta (a cura di), "Codice della privacy e data protection", Giuffrè, 2021

F. Cardarelli (2004) *Il trattamento dei dati personali in ambito pubblico*, in "Il codice dei dati personali. Temi e problemi", Giuffrè, 2004

C. Castaldo (2024), *Libertà individuali e open data. Gli obblighi di servizio pubblico nella gestione dei dati*, Giappichelli, 2024

G.P. Cirillo (a cura di) (2004), *Il codice sulla protezione dei dati personali*, Giuffrè, 2004

A. Corrado (2023), *Il principio di trasparenza e i suoi strumenti di attuazione*, in M.A. Sandulli (a cura di), "Principi e regole dell'azione amministrativa", IV ed., Giuffrè, 2023

G. Corso (2023), *Il principio di legalità*, in M.A. Sandulli (a cura di) "Principi e regole dell'azione amministrativa", IV ed., Giuffrè, 2023

G. Finocchiaro (a cura di) (2017), Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali, Zanichelli, 2017

S. Franca (2023), *I dati personali nell'amministrazione pubblica. Attività di trattamento e tutela del privato*, Editoriale Scientifica, 2023

F. Francario (2023), *Il trattamento dati per finalità di pubblico interesse e l'auspicio di un mutamento d'indirizzo interpretativo*, in "GiustiziaInsieme", 15 settembre 2023

F. Francario (2022), *Protezione dati personali e Pubblica Amministrazione*, in "GiustiziaInsieme", 1° settembre 2021 e in C. Pisani, G. Proia, A. Topo (a cura di) "Privacy e Lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro", vol. II, Giuffrè, 2022

F. Francario (2021), *Disposizioni "urgenti" in materia di protezione dei dati personali. brevi note sul trattamento dati per finalità di pubblico interesse*, in "GiustiziaInsieme", 26 ottobre 2021

I. Genuessi (2024), *Interessi protetti e disciplina del trattamento di dati personale per finalità di pubblico interesse in materia ambientale nell'azione dell'Autorità garante nazionale*, in "Ambientediritto.it", 2024, n. 2

L. Megale (2023), *Il Garante della privacy contro ChatGPT: quale ruolo per le autorità pubbliche nel bilanciare sostegno all'innovazione e tutela dei diritti?,* in "Giornale di diritto amministrativo", 2023, n. 3

F. Modafferri (2021), *Il regime particolare dei trattamenti dati effettuati per l'esecuzione di un compito di interesse pubblici o connesso all'esercizio di pubblici poteri,* in F. Pizzetti, "Protezione dei dati personali in Italia tra GDPR e codice novellato", Giappichelli, 2021

P. Patatini, F. Troncone (a cura di) (2020), *L'oscuramento dei dati personali nei provvedimenti della Corte costituzionale*, Corte Costituzionale, Servizio Studi, dicembre 2020

F. Pizzetti (2021), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Giappichelli, 2021

F. Pizzetti (2016), *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Giappichelli, 2016

B. Ponti (2023), *Attività amministrativa e trattamento dei dati personali. Gli standard di legalità tra tutela e funzionalità*, FrancoAngeli, 2023

S. Rodotà (2007), *Riservatezza*, in "Enciclopedia Giuridica Treccani", VII appendice, 2007

A. Romano Tassone (1996), *Sulla cd "funzione democratica"della motivazione degli atti dei pubblici poteri*, in Aa.Vv. "Studi in onore di Feliciano Benvenuti", IV, Mucchi, 1996 (ora ripubbl. in A. Romano Tassone, "Scritti giuridici", I, Editoriale Scientifica, 2024)

A. Romano Tassone (1987), *Motivazione dei provvedimenti amministrativi e sindacato di legittimità*, Giuffrè, 1987

F. Tigano (2023), *Protezione dati personali e pubblica amministrazione: alcuni spunti di riflessione*, in Aa.Vv., "Studi in onore di C.E. Gallo", Giappichelli, 2023

RIVISTA ITALIANA
DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0259 • articolo sottoposto a peer review • pubblicato in anteprima il 13 gen. 2026

Benedetto Ponti

Trattamento dei dati personali e standard di legalità: elementi di preminenza delle esigenze di circolazione?

Muovendo dai caratteri del meta-principio della finalità del trattamento e dalla clausola di necessarietà, il saggio mostra come il GDPR costruisca uno standard di legalità "funzionale", anche con riferimento ai trattamenti finalizzati all'esecuzione di un compito di interesse pubblico. In ragione del margine di manovra aperto, in materia, dallo stesso GDPR, l'ordinamento italiano è stato invece caratterizzato inizialmente da una disciplina ispirata ad uno *strict legality standard* (che richiedeva una predeterminazione legislativa analitica di dati, operazioni e finalità), per poi allinearsi alla legalità funzionale, in ragione delle modifiche al Codice della privacy introdotte nel 2021. I due standard analizzati comportano un diverso bilanciamento tra esigenze di tutela dei dati personali ed esigenze della loro circolazione. Il saggio si chiude con l'illustrazione di due esempi, uno di rilievo nazionale (le Basi di dati di interesse nazionale nel contesto del PDND) e uno europeo (il Regolamento EHDS), al fine di evidenziare come – più di recente – si vanno affermando strategie normative che, tramite un uso "strategico" delle basi di liceità e del meta-principio di finalità del trattamento, mirano ad incentivare la circolazione e l'uso secondario dei dati personali, segnando una tendenza alla progressiva erosione della centralità del consenso, ed un diverso bilanciamento rispetto alle esigenze di tutela.

GDPR – Circolazione dei dati – Legalità funzionale – Finalità del trattamento – EHDS

Personal data processing and legality standards: evidence of the growing primacy of data free movement?

Starting from the features of the meta-principle of purpose limitation and the necessity clause, the essay shows how the GDPR constructs a functional standard of legality, including with regard to data processing carried out for the performance of a task in the public interest. Given the margin of discretion left by the GDPR in this domain, the Italian legal system was initially characterised by a framework inspired by a strict legality standard (requiring detailed legislative predetermination of data, operations, and purposes), before subsequently aligning with functional legality as a result of the amendments to the Privacy Code introduced in 2021. The two standards analysed entail a different balance between the need to protect personal data and the need to ensure their circulation. The essay concludes by illustrating two examples – one at the national level (the national-interest databases in the context of the PDND) and one at the European level (the EHDS Regulation) – in order to show how, more recently, regulatory strategies have emerged that, through a "strategic" use of lawful bases for data processing and of the meta-principle of purpose limitation, aim to encourage the circulation and secondary use of personal data. These developments signal a trend toward the progressive erosion of the centrality of consent and a shift in the balance between data protection and data-sharing needs.

GDPR – Data free movement – Instrumental legality – Processing purpose – EHDS

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

Questo contributo fa parte della sezione monografica *I dati in ambito pubblico tra esercizio della funzione amministrativa e regolazione del mercato* a cura di Marco Bombardelli, Simone Franca, Anna Simonati

1. Il GDPR: non solo garanzia di protezione, ma anche della circolazione dei dati personali

Come noto, il regolamento generale sulla protezione dei dati personali, entrato in vigore nel 2018, costituisce da allora un punto di riferimento, un *benchmark*, per la tutela dei dati personali[1]. Tuttavia, come spesso la dottrina si è incaricata di ricordare, la *tutela* dei dati personali non costituisce l'oggetto *esclusivo* di quella normativa: infatti, come il primo articolo del regolamento chiarisce (a più riprese), accanto ed in concorrenza con questo obiettivo, il regolamento intende anche assicurare la *libera circolazione* dei dati personali[2]. Le ragioni di questa (apparente) anfibologia sono altrettanto note: definire un quadro di regole, istituti, attori e procedure atte a bilanciare l'esigenza di assicurare tutela ai dati personali (e, per essi, alla libertà, all'autodeterminazione e alla dignità delle persone fisiche), da una parte, e di non ostacolare *oltremisura* lo sviluppo e l'esercizio di tutte quelle attività di carattere economico, politico e sociale che si basano sul trattamento dei dati personali. Il GDPR, detto altrimenti, prende atto del paradigma digitale e di rete, che abilita soluzioni particolarmente economiche, efficaci, potenti (per la produzione di beni, servizi e altre utilità, anche nell'ambito del settore pubblico) e che presuppongono il trattamento dei dati personali: tali soluzioni non devono essere *impedite*, ma piuttosto promosse, in quanto irregimentate/contenute all'interno di un quadro di regole volto ad assicurare un "elevato livello di tutela dei dati personali".

In termini generali, la tutela dei dati riposa innanzitutto nelle *modalità di trattamento*, che devono risultare sempre rispettose dei principi enucleati all'art. 5 del GDPR. I principi, a loro volta, sono plasmati attorno al *meta-principio* che caratterizza l'impianto complessivo di tutela dei dati personali, secondo il modello europeo, così come "precipitato" nel GDPR, principio per il quale il *trattamento* dei dati personali è sempre connesso ad una specifica *finalità*, che ne giustifica la raccolta o la formazione (*ab origine*) e che accompagna tutto il successivo ciclo di trattamento, affinché questo resti *lecito*[3]. E così: la *finalità* costituisce il principale referente rispetto al quale si valuta il rispetto del principio per cui ogni trattamento deve essere *corretto* e *trasparente*; ancora: i trattamenti successivi sono leciti solo se la *finalità* di tali trattamenti è *compatibile* con quella originaria; la *finalità* costituisce il parametro cui si rapporta l'identificazione di quali dati personali sia lecito raccogliere e trattare (principio di *minimizzazione*), ed il tempo per il quale tali dati possono essere conservati (principio di *limitazione della conservazione*). Di più, e preliminarmente (con specifico riferimento, per altro, al principio di *liceità del trattamento*), solo

1. Buttarelli 2016.
2. *Ex multis*: Colapietro 2018; Hoofnagle–Van Der Sloot–Borgesius 2019; Zorzi Galgano 2019-b; Comandè–Schneider 2021; Midiri 2025.
3. Bendiek–Römer 2019.

alcune tipologie di finalità forniscono una base di liceità al trattamento dei dati personali. Si tratta delle finalità che integrano le basi di liceità del trattamento, così come individuate nell'art. 6, eventualmente integrate all'art. 9 da ulteriori requisiti, con riferimento al trattamento dei dati personali cd. "particolari". In assenza (quantomeno) di una di queste basi di liceità, il trattamento è *ipso iure* illecito. Pertanto, si può dire che gli istituti posti a tutela dei dati personali si possono riconoscere – essenzialmente – nell'esistenza di alcune condizioni prescritte dalla legge (dal GDPR) che abilitano il trattamento (e che pertanto, se assenti o carenti, lo impediscono rendendolo *illecito*): tali condizioni attengono ai *presupposti* del trattamento (le basi di liceità) e alle *modalità* del trattamento (i principi sul trattamento), che risultano tutti connessi al meta-principio della finalità del trattamento.

Il rispetto di tali regole costituisce il *meccanismo di protezione dei dati* (per gli interessati), e al tempo stesso (per ciò stesso) un vincolo, *per chi intenda farne uso* (il titolare del trattamento), e pertanto la vigenza di ciascuno di essi (basi e principi) costituisce anche un "ostacolo" alla libera circolazione dei dati.

Ma il GDPR, come detto, non si preoccupa solo di assicurare *tutela* ai dati personali; è inteso anche a favorirne la circolazione. Il primo, fondamentale fattore che opera in questo senso va riconosciuto nella stessa natura della fonte del regolamento europeo. Tale fonte, nella misura in cui è suscettibile di applicarsi direttamente in modo uniforme sul territorio di tutti gli ordinamenti che compongono l'Unione europea (condizione per il vero non sempre realizzata nelle disposizioni del regolamento, come proprio il caso dei trattamenti giustificati dall'esercizio di un compito di interesse pubblico sta a testimoniare), rimuove gli ostacoli (alla circolazione tra gli Stati membri) connessi alla disomogeneità delle tutele assicurate in precedenza (cioè, in vigenza della direttiva 95/46/CE), nei diversi ordinamenti nazionali[4].

Oltre a questo essenziale contributo, nel regolamento si può però identificare un altro fattore che opera nel senso di *favorire* la circolazione. Tale fattore è rappresentato dalla centralità assunta dalla clausola di *necessarietà* come presupposto di liceità del trattamento[5]. Fatta salva la base di liceità che poggia sul consenso dell'interessato (art. 6, lett. a), tutte le basi di liceità disposte dal GDPR poggiano sulla *clausola di necessarietà*. Infatti, è lecito il trattamento che risulti *necessario*, di volta in volta: per l'esecuzione di un contratto di cui l'interessato è parte (lett.b); per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (lett. c); per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica (lett. d); per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (lett. e); per il perseguimento del legittimo interesse del titolare del trattamento o di terzi (lett. f). La clausola di necessarietà risulta quindi *pervasiva*, anche tenuto conto del fatto che – come la dottrina si è incaricata di chiarire, a fronte di alcune inerzie interpretative – il GDPR non instaura alcuna gerarchia di valore o di preferenza tra le diverse basi di liceità[6]. Questo significa che il dato personale, *a prescindere dal consenso dell'interessato*, è autorizzato a circolare (base di liceità) ogniqualvolta il suo trattamento risulti *necessario* ad uno dei fini di cui all'art. 6. La *necessarietà*, dunque, abilita e favorisce la circolazione.

Si noti che, con riferimento alla clausola di necessarietà, il meta-principio della finalità del trattamento opera in modo duplice. Per un verso, coopera nel senso di *incentivare* la circolazione, dal momento che – come detto – la clausola di necessarietà acquista senso con riferimento a questa o quella specifica finalità del trattamento. D'altra parte, tuttavia, gli *usi secondari* dei dati personali (e, quindi, la loro stessa circolazione) sono leciti solo nella misura in cui le finalità per i quali sono effettuati tali *ulteriori trattamenti* risultano non incompatibili con quelle che ne avevano giustificato (in origine) la raccolta. Dunque, la finalità del trattamento opera anche come *limite* alla circolazione.

È all'interno di queste coordinate generali che si propone di leggere la disciplina relativa al trattamento dei dati personali funzionale all'esercizio di funzioni pubbliche.

4. Lin 2024; Chirică 2017; Lynskey 2015.
5. Lindsay 2017; Brouwer 2011; Elgesem 1999.
6. Zorzi Galgano 2019-a; Voigt–Von dem Bussche 2017.

2. Protezione e circolazione dei dati nei trattamenti funzionali all'esercizio delle funzioni pubbliche: quale base di liceità?

Tra le basi di liceità predisposte (e quindi, autorizzate) dal GDPR, quella di cui alla lett. e) dell'art. 6 richiama esplicitamente "l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento", e costituisce pertanto la fattispecie elettiva dalla quale occorre partire per inquadrare il discorso relativo al regime del trattamento dei dati nel caso dell'esercizio di una funzione pubblica. Vale la pena, tuttavia, di verificare se ed in che misura anche le altre basi di liceità potrebbero concorrere a tale fine[7]. Il consenso pare da escludersi, quantomeno tutte le volte in cui il perseguimento di interessi pubblici finisce per radicare in capo al titolare del trattamento una posizione tanto di *potere* quanto di *dovere* tale da risultare incompatibile con i caratteri che devono connotare il consenso (che deve consistere in una "manifestazione di volontà libera", oltre che specifica, informata e inequivocabile dell'interessato). Diversamente, quando l'esercizio di compiti di interesse pubblico si traduce in atti basati che presuppongono il consenso (il contratto, l'accordo), potrebbe risultare plausibile che il trattamento dei dati personali possa appoggiarsi anche su questa base; e tuttavia, anche in questo caso occorre verificare con maggiore attenzione la fattispecie in questione, dal momento che l'esistenza di un atto (finale) perfezionato sulla base di un *accordo* tra l'amministrazione e la parte interessata potrebbe giungere a suggello di uno schema decisionale niente affatto paritario, né del tutto libero. Si pensi, per fare un solo esempio, all'accordo di cui all'art. 11 della legge 241/1990, che costituisce sempre una modalità alternativa di conclusione del procedimento rispetto all'adozione di un provvedimento unilaterale, nel quale l'amministrazione potrebbe, invece, scegliere di spendere il suo potere asimmetrico e unilaterale. Pertanto, affinché la base di liceità fondata sul consenso possa supportare l'esercizio di una funzione amministrativa, occorre non solo che questa si perfezioni in un atto fondato sull'incontro tra la volontà delle parti (a valle), ma anche che (a monte) non sia configurabile – in capo all'amministrazione – una situazione di potere. Tutte le volte, cioè, in cui l'amministrazione agisca (e debba agire) con strumenti di diritto privato, quali il contratto. Ma, in questi casi, la liceità del trattamento dei dati è già prevista (e delimitata) dalla diversa base di liceità di cui all'art. 6, co. 1, lett. b).

La base di liceità di cui alla lett. c) (trattamento necessario per "adempiere un obbligo legale al quale è soggetto il titolare del trattamento") costituisce invece un presupposto applicabile all'esercizio di compiti assegnati ad amministrazioni pubbliche per il perseguimento di interessi pubblici, come confermato dalla giurisprudenza della Corte di giustizia. Tuttavia, si tratta di una fattispecie in cui l'amministrazione si trova astretta in una condizione di vincolo (l'adempimento di un obbligo legale) tale da renderla quasi indistinguibile (sotto il profilo del regime applicabile) da un soggetto di diritto comune (che fosse astretto a consimile vincolo, come accade più di frequente); inoltre, tale base di liceità presuppone un forte grado di predeterminazione del trattamento (quali dati, quali operazioni, per quali finalità) con la conseguenza che il relativo regime è quasi integralmente assorbito nella fattispecie legislativa che disciplina l'obbligo. Insomma, si tratterebbe di *attività vincolata*, ciò che pare escludere l'assegnazione di un potere discrezionale applicabile (anche) alle modalità di trattamento dei dati personali.

Analogo sarebbe il ragionamento con riferimento alla base di liceità di cui all'art. 6, co. 1, lett. d). La "salvaguardia degli interessi vitali dell'interessato" o di altra persona fisica, infatti, è base giuridica idonea ad attivare qualsiasi intervento così giustificato, da chiunque posto in essere, e quindi anche, ma non solo, nell'esercizio di compiti di interesse pubblico. Né il fatto che vi siano articolazioni del pubblico potere esplicitamente e stabilmente dedicate a fronteggiare situazioni di urgenza ed emergenza appare altrimenti dirimente. Infatti, secondo la giurisprudenza, la base di cui alla lett. d) va interpretata in modo *restrittivo*, facendo riferimento a casi come incidenti gravi, emergenze mediche o disastri naturali in cui occorre trattare dati per proteggere la vita

7. Sul punto, vedi *amplius*: Franca 2023; Ponti 2023-a; Niger 2022; Francario 2022; Carullo 2020.

o l'incolumità e non vi è tempo o modo di raccogliere il consenso *o fare affidamento su altra base*[8].

Infine, è lo stesso GDPR ad escludere che la base di liceità connessa al perseguimento del legittimo interesse del titolare del trattamento (art. 6, co. 1, lett. f) sia applicabile ai trattamenti di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti. Una statuizione preziosa, perché esplicita e corrobora (in negativo) il presupposto di liceità di cui alla lett. e). Infatti, tale esclusione contribuisce a chiarire che il titolare che effettua trattamenti per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, non persegue interessi che gli sono propri, ma interessi *altrui* (interessi pubblici, generali, della collettività) e che sono affidati alla sua cura, in una condizione ontologicamente *servente* rispetto ad essi.

Anche alla luce di questa sintetica disamina, appare quindi utile concentrarsi sulla base di cui alla lett. e), che si conferma come la base di liceità più rilevante, quanto all'esercizio di poteri e compiti funzionali al perseguimento di interessi pubblici.

3. *Necessary clause* e trattamento dei dati personali per l'esercizio dei compiti di interesse pubblico

Secondo lo *standard legale* fissato nel GDPR, ogni qualvolta Il trattamento di un dato personale (comune[9]) risulta necessario "per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri", quel trattamento è in potenza lecito, fatto salvo il rispetto dei principi di cui all'art. 5. Lo schema legale in questione, dunque, non predetermina gli elementi essenziali del trattamento (quali dati, sottoposti a quale operazione, per quale finalità), né impone che la legge debba farlo. Ciò che rileva, ai fini della liceità del trattamento, è che esso (a prescindere da come sia poi strutturato) risulti *necessario* per l'esecuzione del compito di interesse pubblico. La clausola di necessarietà, applicata in questo modo, costruisce un modello di *legalità* (in relazione al trattamento dei dati personali) che potremmo definire *funzionale*: la liceità del trattamento dipende non dal rispetto di una regola predeterminata che lo disciplina, ma dalla attitudine del trattamento ad assicurare l'esecuzione del compito di interesse pubblico[10]. Entro queste coordinate, la base giuridica rileva (come necessaria) nella misura in cui indica (e deve indicare) quale sia il compito di interesse pubblico, quale sia cioè la finalità, l'interesse alla cui cura il soggetto (tendenzialmente, ma non necessariamente) pubblico è (così) preposto, e solo in questa misura. Ciò ha due ordini di conseguenze principali. Per un verso, la f*inalità del trattamento* (di cui al meta-principio del GDPR) finisce per coincidere con la *finalità dei compiti di interesse pubblico*, e in questo contesto gioca il medesimo (duplice) ruolo che abbiamo tratteggiato in linea generale. Per un verso, la finalità di interesse pubblico *attiva* la circolazione dei dati (il dato può circolare, se la circolazione è necessaria al perseguimenti dell'interesse pubblico); per altro verso, la stessa finalità di interesse pubblico opera come *limite* a questa circolazione, dal momento che, perché il trattamento (secondario) risulti lecito, occorrerà verificare se la finalità in vista della quale tale trattamento viene posto in essere (perché necessario) risulta "non incompatibile" con la finalità che aveva giustificato la raccolta/formazione originaria del dato personale in questione. In secondo luogo, le modalità di trattamento risultano potenzialmente rimesse (anche in modo integrale) alla autonoma determinazione del soggetto "investito" dei compiti di interesse pubblico, il quale è tenuto a *rendere conto* delle scelte compiute in merito (in

8. Cfr. CGUE C252/21 *Meta Platforms Inc. vs Bundeskartellamt*.
9. Lo schema legale per quanto concerne il trattamento dei dati "particolari" (i.e., i "dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona") è ancora modellato sulla clausola di necessarietà, ma è reso più esigente da ulteriori elementi: il trattamento deve essere necessario per dare soddisfazioni a ragioni di interesse pubblico rilevante, così qualificate dal diritto dell'Unione o degli Stati membri; diritto che deve risultare proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (art. 9, co. 2, lett. g).
10. Ponti 2023-a.

accordo con il principio di responsabilizzazione, art. 5, co. 2), scelte che però gli pertengono.

Quali sono, tuttavia, i caratteri che qualificano un trattamento come *necessario*, ai fini dell'esecuzione di un compito di interesse pubblico? L'analisi della giurisprudenza della Corte di giustizia ha consentito di verificare che la *necessarietà* consiste in un rapporto di strumentalità del mezzo impiegato (il trattamento dei dati) rispetto al fine (l'esecuzione del compito di interesse pubblico ovvero l'integrazione della finalità del trattamento), e che detta strumentalità risulta realizzata nella misura in cui il trattamento risulta *efficace* (cioè, idoneo a consentire l'esecuzione del compito di interesse pubblico)[11]. Ora, i trattamenti possono risultare più o meno invasivi della sfera giuridica dell'interessato (in ragione di fattori diversi, quali: la quantità e qualità dei dati personali oggetto di trattamento, la tipologia di operazioni effettuate, i rischi cui sono di conseguenza esposti gli interessati). Sotto questo profilo, la stessa giurisprudenza ha chiarito che, tenuto conto del principio di *minimizzazione*, un trattamento *meno invasivo* risulta necessario, in luogo di un altro, *più invasivo*, solo se e nella misura in cui risulti *altrettanto efficace* nel perseguire l'interesse pubblico. Questa notazione ci consente di identificare quale sia il bilanciamento tra esigenze di tutela e esigenze di circolazione realizzato mediante la codificazione della clausola di necessarietà applicata ai trattamenti strumentali all'esercizio di funzioni pubbliche. Tale clausola, infatti, sconta di per sé effetti di compressione o sacrificio delle esigenze di tutela, e che coincidono con gli effetti determinati da tutti i trattamenti dei dati personali che risultano *strumentali* al perseguimento di una finalità pubblica, dato un certo livello di efficacia della soluzione impiegata. Pertanto, a conferma della natura funzionale dello standard di legalità connesso alla clausola di necessarietà, è l'*efficacia del trattamento* applicato ai dati personali la misura che lega in termini di proporzionalità l'equilibrio (adattabile, non predeterminato) che si realizza tra esigenze di tutela ed esigenze di circolazione[12].

4. Margini di manovra e *strict legality standard*

Lo standard di *legalità funzionale* posto dal GDPR non è però l'unico che può regolare il trattamento dei dati personali per l'esercizio di funzioni pubbliche. Infatti, la disciplina eurounitaria, *in parte qua* apre uno spazio agli Stati membri per introdurre (o mantenere) una disciplina interna utile ad adattare il quadro normativo del GDPR. Origini e ragioni di questa clausola di adattamento sono state indagate altrove; basti qui chiarire che essa si giustifica anche perché consente agli ordinamenti di potersi "distaccare" dallo standard della *legalità funzionale*, anche per tenere conto delle tradizioni e delle caratteristiche del diritto amministrativo interno. Come noto, è (stato) questo il caso anche dell'ordinamento nazionale italiano che, per il periodo compreso tra l'entrata in vigore della disciplina interna di adeguamento al GDPR (agosto 2018) e le modifiche al Codice della privacy introdotte a seguito del c.d. decreto "capienze" (ottobre 2021), ha sperimentato un diverso standard legale, per come definito dalle disposizioni (per come allora formulate) agli art. 2-*ter* e seguenti. Tale disciplina, anche in virtù della interpretazione che ne aveva fatto il Garante della privacy, imponeva (invece) che il trattamento dei dati personali (operato per il perseguimento di interessi pubblici) fosse predeterminato da una norma di legge (o di regolamento, ma di carattere meramente esecutivo) quanto a: la tipologia di dati da trattare, il tipo di operazioni da effettuarsi, la finalità da perseguire. Dunque, una *strict legality rule*, nella quale si realizza un (ben diverso bilanciamento) tra esigenze di circolazione ed esigenze di tutela. Le seconde

11. Ponti, 2023-a.

12. Fa eccezione (sempre nella giurisprudenza della Corte di giustizia) l'ipotesi dello specifico trattamento che consista nella *pubblicazione* dei dati personali. Infatti, la diffusione al pubblico dei dati personali rappresenta una tipologia di trattamento idonea a determinare un pregiudizio così grave e intenso da modificare i temini del giudizio di proporzionalità, che trasmuta in giudizio di *stretta indispensabilità*. Secondo questa regola di bilanciamento, non solo tale trattamento deve essere previsto esplicitamente dal legislatore, ma esso risulta comunque incompatibile con il GDPR qualora sia astrattamente disponibile e concretamente sperimentabile una diversa soluzione, basata su un diverso (e meno invasivo) trattamento dei dati personali, *anche se meno efficace*: cfr. Ponti 2023-a; CGUE C-184/20, *Vyriausioji tarnybinės etikos komisija*.

appaiono più pienamente assecondate, nella misura in cui è il legislatore a dover autorizzare in modo esplicito, rigido e analitico le specifiche modalità di trattamento dei dati personali; le prime, invece, risultano maggiormente sacrificate, dal momento che – in assenza di una specifica previsione legislativa – il trattamento dei dati (che pure risulti funzionale al perseguimento dell'interesse pubblico) risulta interdetto. Un regime di *legalità funzionale* "temperata", tuttavia, era applicato al caso della *circolazione* dei dati *tra diverse amministrazioni*: in questo caso, la mancata previsione dello scambio dei dati – che pure risultasse necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali – era possibile, sebbene comunque soggetto ad un onere di notificazione al Garante[13].

A seguito delle modifiche introdotte nell'autunno del 2021, il quadro nazionale italiano è stato profondamente modificato, ed appare oggi sostanzialmente allineato allo standard della *legalità funzionale*, così come disposto nel GDPR. Infatti, non solo alle amministrazioni è stato assicurato il potere di disciplinare i trattamenti con propri atti organizzativi (anche in assenza di una autorizzazione legislativa[14]), ma ad esse è *comunque* accordata la possibilità di effettuare i trattamenti dei dati personali (compresa la circolazione dei dati all'interno del settore pubblico) che risultino *necessari* per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri loro attribuiti[15]. Rimane ferma, però, l'eccezione relativa al trattamento che consiste nella pubblicazione dei dati personali (anche quando funzionale all'assolvimento di compiti di interesse pubblico), che richiede una apposita norma legislativa che lo preveda, secondo l'interpretazione offerta dal Garante[16].

5. Strategie legislative per la circolazione dei dati

Come detto, il meta-principio della finalità del trattamento opera (anche) come limite alla circolazione dei dati personali, dal momento che il (conseguente) principio di *limitazione della finalità* impone che i trattamenti secondari siano effettuati per finalità *non incompatibili* con quelle che hanno giustificato la raccolta/formazione originaria del dato personale in questione. Rispetto a questo *elemento strutturale*, che costituisce una matrice identificativa del modello europeo di tutela dei dati, i legislatori hanno utilizzato in *modo strategico* la leva normativa, per ovviare all'intrinseco effetto di limitazione alla circolazione che ne deriva.

Un paio di esempi possono essere sufficienti, al fine di rappresentare come le esigenze di circolazione e di condivisione dell'informazione, all'interno del settore pubblico (e tra settori pubblici di differenti Stati membri dell'Unione europea, come si dirà tra poco), stanno portando a "forzare" le logiche del GDPR.

Un primo esempio è tratto dal contesto nazionale italiano e fa riferimento a quelle banche dati in cui sono raccolte e organizzate categorie omogenee di informazioni allo scopo precipuo di rendere

13. A seguito della notificazione, la comunicazione dei dati da una amministrazione all'altra poteva avere inizio solo decorsi quarantacinque giorni, senza che il Garante fosse intervenuto prescrivendo delle misure *a garanzia degli interessati*.
14. Cfr. l'art. 2-*ter*, co. 1 del Codice privacy attualmente vigente, per effetto delle modifiche introdotte dal d.l. 139/2021, convertito in legge 205/2021.
15. Cfr. l'art. 2-*ter*, co. 1-*bis* del Codice privacy. Appaiono quindi non del tutto condivisibili le preoccupazioni espresse in dottrina, laddove si prospetta *l'incompatibilità* del quadro normativo nazionale (come risultante dalle modifiche introdotte nel 2021) rispetto a quello europeo (cfr. Carullo 2024). Infatti, il citato comma 1-*bis* dell'art. 2-*ter* del Codice privacy non fa che riprodurre (in termini quasi letterali) lo standard legale di cui all'art. 6, co. 1, lett. e) del GDPR; pertanto, le obiezioni richiamate andrebbero semmai indirizzate al regolamento, e dovrebbero concernere lo *standard di legalità funzionale* da esso introdotto, nella misura in cui non appare del tutto in linea con le esigenze imposte dalla vigenza – sul piano interno – del principio di legalità, in quanto applicato al trattamento dei dati personali. Sul punto – oltre al contributo di Francario, in questo numero della Rivista (Francario 2025) – cfr. anche Franca 2023.
16. Cfr., *ex multis*, il provvedimento dell'11 aprile 2024, doc. web n. 10019523 e il Provvedimento del 24 gennaio 2024, doc. web n. 9987578.

tali informazioni disponibili al sistema pubblico nel suo complesso, e a ciascuna delle sue componenti, al fine di alimentare l'esercizio delle rispettive funzioni amministrative; quelle *basi di dati di interesse nazionale*, disciplinate agli artt. 60 e ss. del Codice dell'amministrazione digitale. Il legislatore utilizza in modo strategico il meta-principio di finalità, poiché assegna in modo esplicito alla banca dati *il compito di raccogliere, conservare determinate informazioni per renderle disponili alle altre amministrazioni*. Così facendo, l'intervento legislativo (che costituisce e/o qualifica la base di dati di interesse nazionale) "spezza" la catena di valutazioni circa la *compatibilità* tra le finalità originaria della raccolta e le finalità dei successivi trattamenti secondari. La raccolta, la conservazione e l'allineamento delle informazioni, compresi i dati personali, che vanno a costituire la specifica *base di dati*, sono trattamenti che *ab initio* hanno *la finalità* di rendere le informazioni utili e disponibili alla circolazione, così che la successiva valutazione di compatibilità (rispetto al trattamento posto in essere dall'amministrazione che fruisce del servizio di "erogazione dei dati") avrà *sempre* esito positivo, *by design*. In questo modo, il principio di limitazione della finalità è utilizzato per devitalizzarne la componente *di tutela* e per esaltarne la componente *di circolazione*. Non deve sfuggire la circostanza per cui questo meccanismo può operare anche in virtù del *margine di manovra* aperto alle legislazioni nazionali dall'art. 6, commi 2 e 3 del GDPR; in particolare, è il comma 3 che consente ai legislatori (degli Stati membri e dell'Unione) di introdurre "disposizioni specifiche per adeguare l'applicazione delle norme del regolamento", anche per quanto riguarda "le limitazioni della finalità".

Non è quindi casuale che, nel momento in cui – anche per effetto della spinta impressa dal PNRR – si è proceduto a edificare e mettere in opera una infrastruttura tecnica capace *effettivamente* di far circolare le informazioni all'interno del sistema pubblico (la Piattaforma digitale nazionale dei dati – PDND), le prime banche dati designate per essere integrate nel sistema sono state proprio le Basi di dati di interesse nazionale[17]: il presupposto normativo volto a favorire la circolazione dei dati (anche personali) all'interno del sistema pubblico ha così trovato riscontro in una soluzione volta a consentire *effettivamente* (sul piano tecnico ed organizzativo) la circolazione dei dati[18].

Un secondo esempio è rappresentato dalla strategia perseguita a livello europeo, volta a porre rimedio agli ostacoli alla circolazione dei dati sanitari, ostacoli determinati dalla frammentazione dei regimi giuridici nazionali, anche in ragione delle clausole di apertura a discipline nazionali contenute nell'art. 9 del GDPR (e che si aggiungono a quelle di cui all'art. 6, commi 2 e 3 di cui si è già detto)[19]. Il recentissimo *Regolamento sullo spazio europeo dei dati sanitari*-EHDS[20], infatti, utilizza la leva di una normativa *ad hoc* (di livello unionale) al fine di fornire le basi giuridiche utili ad assicurare che i dati sanitari possano circolare all'interno dell'Unione, così da promuovere una serie di finalità, identificate all'art. 53 del regolamento[21]. Il Regolamento EHDS (come descritto in modo

17. Come previsto dall'art. 50-*ter*, comma 2 del Codice dell'amministrazione digitale, così come integrato dal d.l. 77/2021, "In fase di prima applicazione, la Piattaforma [digitale nazionale dei dati, ndr] assicura prioritariamente l'interoperabilità con le basi dati di interesse nazionale".

18. Ponti 2023-b.

19. Quinn–Ellyne–Yao 2024.

20. Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio, dell'11 febbraio 2025, sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847.

21. Le finalità che il regolamento promuove possono essere sintetizzate come segue: cura del pubblico interesse nell'ambito della sanità pubblica o della medicina del lavoro, come nel caso delle attività per la protezione da gravi minacce per la salute a carattere transfrontaliero, della sorveglianza della sanità pubblica o delle attività per la garanzia di elevati livelli di qualità e sicurezza dell'assistenza sanitaria, inclusa la sicurezza dei pazienti, e di medicinali o dispositivi medici pubblico interesse nell'ambito della sanità pubblica o della medicina del lavoro; definizione delle politiche nel settore sanitario o dell'assistenza; statistiche relative al settore sanitario o dell'assistenza; istruzione o insegnamento nel settore sanitario o dell'assistenza al livello della formazione professionale o dell'istruzione superiore; ricerca scientifica nel settore sanitario o dell'assistenza che contribuisce

analitico nel considerando 52) fa un uso *strategico* delle basi giuridiche così come identificate nel GDPR. Per un verso, utilizza la base di cui all'art. 6, par. 1, lett. c), completa dei requisiti aggiuntivi di cui all'art. 9, par. 2, lett. i) e j), per rendere obbligatoria la comunicazione/messa a disposizione dei dati sanitari (che rientrano nelle categorie di dati identificati all'art. 51) da parte dei soggetti qualificati come "Titolari dei dati sanitari" (art. 60). Utilizza, poi, la base di cui all'art. 6, par. 1, lett. e), completa dei requisiti aggiuntivi di cui all'art. 9, par. 2, lett. da g) a j), per assegnare ai costituendi/designandi "Organismi responsabili dell'accesso ai dati sanitari" (artt. 55, 57-59) *i compiti di interesse pubblico*, che consistono nella gestione dell'accesso ai dati resi disponibili dai titolari dei dati sanitari. In particolare, tra i molti compiti assegnati, spiccano quelli di decisione sulle domande di accesso ai dati sanitari (presentate dagli "Utenti dei dati sanitari") e la conseguente autorizzazione all'accesso a tali dati presso i rispettivi titolari (art. 57, par. 1, lett. a); nonché la pubblicazione e l'aggiornamento di una serie di informazioni utili a consentire la circolazione dei dati sanitari e a dare conto dei risultati conseguiti dagli utenti (art. 57, par. 1, lett. j)[22]. Sulla base di questa infrastruttura di *governance*, gli "Utenti dei dati sanitari", purché dotati di una base giuridica prevista dall'articolo 6, par. 1, lett. e), o f), possono presentare richieste di accesso e di autorizzazione all'uso secondario e – qualora autorizzati – utilizzare i dati sanitari che già assicurano il rispetto delle condizioni di cui all'art. 9, par. 2. A tale fine, il regolamento impedisce agli Stati membri di introdurre condizioni ulteriori (compreso il consenso dell'interessato) per l'uso secondario, se non a limitati fini e solo per alcune tipologie di dati personali[23].

Anche qui, l'uso strategico della leva normativa è utile a *svincolare* il dato sanitario (personale) dalla (specifica) finalità connessa alle ragioni della sua originaria raccolta e trattamento, e renderlo disponibile agli *utenti secondari* già caratterizzato da finalità ulteriori e diverse, così che il trattamento *ulteriore* di questi dati sarà (sempre) *lecito*, nella misura in cui (al netto del rispetto delle prescrizioni del regolamento EHDS) tali trattamenti risultino compatibili con le finalità esplicitamente selezionate e qualificate[24] dal regolamento stesso.

Il meccanismo di incentivazione dell'uso secondario dei dati sanitari abilitato dall'EHDS è

alla sanità pubblica o alla valutazione delle tecnologie sanitarie; miglioramento ed ottimizzazione della prestazione di assistenza sanitaria.

22. Gli organismi responsabili dell'accesso ai dati sanitari devono pubblicare, tra le altre cose: un catalogo nazionale contenente informazioni dettagliate sulla fonte e sulla natura dei dati sanitari elettronici e sulle condizioni per la loro messa a disposizione; le domande di accesso ai dati sanitari; tutte le autorizzazioni ai dati rilasciate o le richieste di dati sanitari approvate come pure le decisioni di diniego, unitamente alla relativa motivazione; i risultati o gli esiti dell'uso secondario comunicati dagli utenti dei dati sanitari.
23. Se il considerando 52, a questo fine, suggerisce che "Stati membri non dovrebbero più poter mantenere o introdurre, a norma dell'articolo 9, paragrafo 4, del regolamento (UE) 2016/679, ulteriori condizioni, comprese limitazioni e disposizioni specifiche che richiedono il consenso delle persone fisiche, per quanto riguarda il trattamento per l'uso secondario dei dati sanitari elettronici personali a norma del presente regolamento, ad eccezione dell'introduzione di misure più rigorose e garanzie supplementari a livello nazionale intese a tutelare la sensibilità e il valore di taluni dati come previsto dal presente regolamento", l'articolato dispone (di conseguenza) che agli Stati membri è consentito introdurre misure più rigorose e garanzie supplementari a livello nazionale solo se intese a tutelare la sensibilità e il valore dei dati, e solo relativamente a dati ricompresi entro alcune categorie di dati sanitari, ossia: i dati genetici, epigenomici e genomici umani; altri dati molecolari umani; i dati provenienti dalle applicazioni per il benessere; nonché dati sanitari provenienti da biobanche e banche dati associate (cfr. art. 51, par. 4).
24. L'art. 53 identifica tali finalità in modo particolarmente ampio, non solo con riferimento alla numerosità delle casistiche previste (lett. da a) a f) dell'art. 53, par. 1), ma anche con riferimento alle modalità con le quali ciascuna di queste finalità è stata formulata. Ciò che, anche a parere dei primi commentatori della disciplina appare una forzatura del modello di tutela di cui al GDPR, in ragione della enorme discrezionalità che appare rimessa in capo agli Organismi responsabili dell'accesso ai dati sanitari nell'autorizzare l'uso secondario dei dati sanitari elettronici: cfr. Quinn–Ellyne–Yao 2024.

di recentissima introduzione, ed occorre ancora capire se ed in che misura sarà efficace: in termini simili a quelli già visti nel primo esempio, tale *effettività* passa non solo per la abilitazione di un quadro normativo idoneo a consentire la circolazione dei dati[25], ma anche dalla realizzazione di una coerente infrastruttura tecnica. Infatti, l'EHDS intende costruire uno spazio per la circolazione dei dati sanitari *elettronici*, ed una parte significativa del regolamento è dedicata a realizzare anche i presupposti *tecnologici* necessari a tale fine, ossia ad assicurare che i dati raccolti (in sede di uso primario) siano codificati in modo tale, poi, da risultare *interoperabili*. Uno sforzo di armonizzazione e coordinamento tecnico non meno impegnativo rispetto a quello di carattere legale[26].

Entrambi gli esempi analizzati indicano una più recente prevalenza delle esigenze di circolazione, che si realizzano mediante una modificazione del modo in cui tali esigenze si combinano con quelle di tutela dei dati personali. Tale prevalenza opera, in particolare, lungo due direttrici. Per un verso, attraverso la perdita di centralità del consenso, come base di legittimazione del trattamento dei dati personali, a favore delle altre basi di liceità previste dal GDPR, fondate invece sulla clausola di necessarietà e – per conseguenza – sulla versione *funzionale* dello *standard di legalità*. Per altro verso, per un uso strategico della *leva normativa primaria* (a livello nazionale o europeo), mediante la quale il meta-principio della finalità del trattamento (che non viene rinnegato, né abbandonato) è (piuttosto) impiegato al fine di esaltare le sue ricadute in termini di *abilitazione della circolazione dei dati*, e per attenuare fin dove possibile le (opposte) ricadute in termini di tutela dell'interessato. Non appaia paradossale osservare come, in questo movimento, la fonte legislativa primaria finisca per essere utilizzata a ridimensionare le esigenze più garantiste del principio di legalità.

Riferimenti bibliografici

R. Becker, D. Chokoshvili, E.S. Dove (2024), *Legal bases for effective secondary use of health and genetic data in the EU: time for new legislative solutions to better harmonize data for cross-border sharing?*, in "International Data Privacy Law", vol. 14, 2024, n. 3

A. Bendiek, M. Römer (2019), *Externalizing Europe: the global effects of European data protection*, in "Digital Policy, Regulation and Governance", vol. 21, 2019, n. 1

E.R. Brouwer (2011), *Legality and data protection law: The forgotten purpose of purpose limitation*, in L.F.M. Besselink, F. Pennings, S. Prechal (eds.),"The eclipse of the legality principle in the European Union", Kluwer Law International, 2011

G. Buttarelli (2016), *The EU GDPR as a clarion call for a new global digital gold standard*, in "International Data Privacy Law", vol. 6, 2016, n. 2

G. Carullo (2024), *Dati personali e fini pubblici: dubbi di compatibilità europea del Codice Privacy*, in "CERIDAP", 2024, n. 3

G. Carullo (2020), *Trattamento di dati personali da parte delle pubbliche amministrazioni e natura del rapporto giuridico con l'interessato*, in "Rivista italiana di diritto pubblico comunitario", 2020, 1-2

S. Chirică (2017), *The main novelties and implications of the new general data protection regulation*, in "Perspectives of business law journal", vol. 6, 2017

25. Sulla incompletezza di tale quadro giuridico, con rifermento a talune fasi del trattamento e a talune categorie di utenti dei dati sanitari, cfr. Becker–Chokoshvili–Dove 2024.

26. Cfr. il Capo II (Uso primario), Sezione 3 (Infrastruttura transfrontaliera per l'uso primario dei dati sanitari elettronici personali), nonché l'intero Capo III (Sistemi di cartelle cliniche elettroniche e applicazioni per il benessere) del Regolamento EHDS.

G.D. Colapietro (2018), *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in "federalismi.it", 2018, n. 22

G. Comandè, G. Schneider (2021), *Can the GDPR make data flow for research easier? Yes it can, by differentiating! A careful reading of the GDPR shows how EU data protection law leaves open some significant flexibilities for data protection-sound research activities*, in "Computer Law & Security Review", vol. 41, 2021

D. Elgesem (1999), *The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data*, in "Ethics and Information Technology", vol. 1, 1999, n. 4

S. Franca (2023), *I dati personali nell'amministrazione pubblica: attività di trattamento e tutela del privato*, Università degli Studi di Trento, 2023

F. Francario (2025), *Il trattamento dei dati personali per finalità d'interesse pubblico*, in "Rivista italiana di informatica e diritto", 2025, n. 2

F. Francario (2022), *Protezione dati personali e Pubblica Amministrazione*, in "GiustiziaInsieme", 1° settembre 2021 e in C. Pisani, G. Proia, A. Topo (a cura di) "Privacy e Lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro", vol. II, Giuffrè, 2022

C.J. Hoofnagle, B. Van Der Sloot, F.Z. Borgesius (2019), *The European Union general data protection regulation: what it is and what it means*, in "Information & Communications Technology Law", vol. 28, 2019, n. 1

Y. Lin (2024), *More Than an Enforcement Problem: The General Data Protection Regulation, Legal Fragmentation, and Transnational Data Governance*, in "Columbia Journal of Transnational Law", vol. 62, 2024, n. 1

D. Lindsay (2017), *The Role of Proportionality in Assessing Trans-Atlantic Flows of Personal Data*, in D.J.B. Svantesson, D. Kloza (eds.), "Trans-Atlantic Data Privacy Relations as a Challenge for Democracy", European Integration and Democracy Series. Intersentia, 2017

O. Lynskey (2015), *The foundations of EU data protection law*, Oxford University Press, 2015

F. Midiri (2025), *Il ruolo delle autorità indipendenti nella regolazione del trattamento dei dati*, in "Rivista italiana di informatica e diritto", 2025, n. 2

S. Niger (2022), *La protezione dei dati personali nella pubblica amministrazione. L'esperienza italiana*, in "European review of digital administration & law", vol. 3, 2022, n. 2

S. Orlando (2024), *Sulla necessità di un controllo di liceità sostanziale per tutte le basi del trattamento dei dati personali*, in "Persona e mercato", 2024, n. 3

B. Ponti (2023-a), *Attività amministrativa e trattamento dei dati personali: gli standard di legalità tra tutela e funzionalità*, FrancoAngeli, 2023

B. Ponti (2023-b), *Tre scenari di digitalizzazione amministrativa "complessa": dalla interoperabilità predicata alla standardizzazione praticata*, in "Istituzioni del federalismo: rivista di studi giuridici e politici", 2023, n. 3

P. Quinn, E. Ellyne, C. Yao (2024), *Will the GDPR Restrain Health Data Access Bodies Under the European Health Data Space (EHDS)?*,in "Computer Law & Security Review", vol. 54, 2024

P. Voigt, A. Von dem Bussche (2017), *The EU general data protection regulation (GDPR). A practical guide*, 1st edition, Springer, 2017

N. Zorzi Galgano (2019-a), *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, 2019

N. Zorzi Galgano (2019-b), *Le due anime del GDPR e la tutela del diritto alla privacy*, in "Persona e mercato dei dati. Riflessioni sul GDPR", Cedam, 2019

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0247 • articolo sottoposto a peer review • pubblicato in anteprima il 21 nov. 2025

Stefano Corso

Il trattamento dei dati personali in ambito sanitario

Il trattamento dei dati personali in ambito sanitario è regolato da plurime disposizioni appartenenti a fonti di diverso livello. Uno dei principali aspetti che connota questa disciplina attiene alla tipologia di dati personali maggiormente trattati nella sanità, ossia i dati relativi alla salute. Da un esame complessivo della normativa, nazionale e sovranazionale, emerge la tensione fra gli interessi sottesi – di natura pubblica e privata – di cui il legislatore cerca di realizzare un bilanciamento. Elemento caratteristico del rinnovato quadro giuridico è il superamento definitivo della regola del consenso con l'approdo a paradigmi differenti di protezione dei dati, che possano valorizzare effettivamente la dimensione circolatoria del fenomeno. Nel cangiante panorama legislativo in materia di dati sanitari, permane la garanzia del diritto fondamentale della persona all'autodeterminazione. L'istituzione dello spazio europeo dei dati sanitari conferma l'assunto.

Protezione dei dati personali – Trattamento di dati relativi alla salute – Autodeterminazione
Fascicolo sanitario elettronico – Spazio europeo dei dati sanitari

The processing of personal data in healthcare

The processing of personal data in the healthcare sector is governed by multiple provisions from various sources. One of the main aspects of this regulation concerns the type of personal data most commonly processed in healthcare: data concerning health. An examination of national and supranational legislation reveals underlying tensions between public and private interests, which the legislator must balance. A defining feature of the updated legal framework is the definitive shift away from the consent rule, with different data protection paradigms now in place that can effectively enhance the circulation of data. Despite the changing legislative landscape regarding health data, individuals' fundamental right to self-determination remains guaranteed. The establishment of the European Health Data Space confirms this assumption.

Personal data protection – Processing of data concerning health – Self-determination
Electronic Health Record – European Health Data Space

L'Autore è assegnista di ricerca in Diritto privato presso il Dipartimento di Scienze politiche, giuridiche e studi internazionali dell'Università di Padova

Questo contributo fa parte della sezione monografica *I dati in ambito pubblico tra esercizio della funzione amministrativa e regolazione del mercato*, a cura di Marco Bombardelli, Simone Franca, Anna Simonati

1. Autodeterminazione terapeutica e autodeterminazione informativa

"La dignità, l'identità, la libertà e l'autodeterminazione, la privacy nei suoi diversi significati sono prerogative da declinare con la specificazione '*nel corpo*'"[1]. Con queste parole Paolo Zatti si riferiva alle situazioni giuridiche pertinenti alla persona rapportandole al corpo. E Stefano Rodotà, citando queste stesse parole, aggiungeva: "dunque nella vita"[2]. Il ragionamento portava alla contrapposizione dell'autonomia del soggetto nei rapporti patrimoniali rispetto all'autonomia nelle scelte esistenziali. L'autodeterminazione come diritto della persona si declina così come autodeterminazione terapeutica. Ma non è questo l'unico modo possibile di concepire l'autodeterminazione.

Il 15 dicembre 1983, nel celebre *Volkszählungsurteil*, la Corte costituzionale tedesca[3] sancì, com'è noto, il diritto all'autodeterminazione informativa e tale diritto fu ancorato agli artt. 1 e 2 del *Grundgesetz*, riconducendosi direttamente all'istituto dell'*allgemeines Persönlichkeitsrecht*[4]. L'autodeterminazione informativa venne così intesa come il diritto fondamentale della persona di decidere autonomamente in merito alla divulgazione e all'utilizzo dei propri dati personali, derivante dal principio cardine della dignità e dalla garanzia del libero sviluppo della personalità, che richiede la protezione dell'individuo dalla raccolta, la conservazione, l'uso e la diffusione illimitati dei suoi dati personali.

Quando si parla di autodeterminazione in ambito sanitario, tuttavia, non è a quella informativa che si fa usualmente riferimento, bensì all'autodeterminazione terapeutica o meglio, e più in generale, all'autodeterminazione della persona sul proprio corpo. L'autodeterminazione accede, da questo piano, a un insieme di significati ampio e diversificato, una parte dei quali si rispecchia nei corrispondenti significati che stanno sul piano dell'autodeterminazione informativa e un'altra

1. Zatti 2009, p. 86.
2. Rodotà 2010, p. 211.
3. BVerfG, 15.12.1983, in "Neue Juristische Wochenschrift", 1984, p. 419.
4. Tale correlazione fu poi ribadita dall'art. 1 del *Bundesdatenschutzgesetz* del 1990 (e successive modifiche) nonché dalle normative dei singoli *Länder*. Resta 2006, p. 572.

parte, la più cospicua, vi è invece ignota. Nell'ordinamento italiano l'autodeterminazione, in questo senso, ma non solo, è considerata oggetto di un diritto fondamentale della persona, che trova il suo punto di sintesi con il diritto alla salute, nel consenso informato del paziente. Il consenso informato al trattamento sanitario è elemento fondamentale del diritto all'autodeterminazione terapeutica della persona, annoverabile fra i diritti della personalità, e la sua violazione determina il diritto al risarcimento del danno[5].

La consensualità nella relazione di cura, con l'abbandono dell'impostazione verticale e paternalistica del rapporto classico medico-paziente e con la centralità della persona in medicina, ha trovato riconoscimento normativo nella legge 22 dicembre 2017, n. 219[6]. Rubricata "Norme in materia di consenso informato e di disposizioni anticipate di trattamento", la legge 219/2017 è giunta a delineare una disciplina per la relazione di cura, dal momento attuale del dialogo fra medico e paziente a quello finale, in cui un'attualità di quel dialogo può venire a mancare, per le condizioni di fragilità dell'individuo. La legge non ha riempito un'area vuota di diritto, ma si è innestata su un terreno già abitato dal diritto vivente, nel fertile scambio di dottrina e giurisprudenza[7].

Il *consenso informato* – espressione di cui si fa uso anche nella legge 219/2017 – è l'elemento che connota tanto l'autodeterminazione terapeutica quanto l'autodeterminazione informativa, ritrovando l'autodeterminazione, come comun denominatore, il profilo della volontà del soggetto. All'interno del contesto sanitario, nel percorso di cura, l'autodeterminazione terapeutica supera e, per così dire, assorbe quella informativa. Infatti, nel momento in cui l'individuo esprime consapevolmente il proprio consenso al trattamento sanitario, non è necessario – come si ricava dall'art. 9 del Regolamento generale sulla protezione dei dati (reg. Ue n. 679 del 2016, c.d. GDPR)[8] – che egli manifesti pure il consenso al trattamento dei suoi dati, perché questo avvenga.

Uno degli aspetti critici della disciplina italiana in materia, prima che entrasse in vigore e fosse applicabile il GDPR, era proprio questo. Dover richiedere il consenso del paziente al trattamento dei suoi dati sanitari per l'esecuzione della prestazione sanitaria apriva, in astratto, all'aporia del soggetto che avrebbe potuto domandare la prestazione medica, quindi acconsentendo al trattamento sanitario, e allo stesso tempo negare il consenso al trattamento dei dati relativi alla propria salute. In concreto, per ottenere la prestazione medica, il paziente ovviamente acconsente anche al trattamento dei suoi dati sanitari e allora si comprende come il consenso possa dirsi del tutto apparente o necessitato[9].

L'autodeterminazione informativa in ambito sanitario non è stata tuttavia obliterata. Deve ritenersi, infatti, che essa sia recuperata proprio nella dimensione della relazione di cura, sul piano del rapporto medico-paziente, non più gerarchizzato secondo gli schemi del passato, ma costruito sul dialogo e orientato all'alleanza terapeutica[10].

Alla luce del ruolo che continua a svolgere il consenso informato tanto sul piano del trattamento sanitario quanto su quello del trattamento dei dati personali e, nella specie, nell'ambito sanitario, sembra potersi intravedere un parallelismo, seppure imperfetto, fra autodeterminazione come governo del corpo e autodeterminazione come controllo delle proprie informazioni: governo del corpo fisico e governo del corpo digitale. L'osservazione si arricchisce con riferimento alla protezione dei dati personali alla luce delle varie situazioni giuridiche riconosciute attraverso i c.d. "diritti dell'interessato".

L'autodeterminazione informativa nel contesto sanitario si connota specialmente per due aspetti: la sensibilità dei dati personali coinvolti e la qualifica prevalentemente pubblica dei

5. Pucella 2010. Cfr. Calderai 2015, p. 225 ss. Spec. con riferimento alla prospettiva del diritto sanitario, v. Pioggia 2011, p. 127 ss.
6. Su tutti, Zatti 2018, p. 247 ss.; Zatti 2019, p. 3 ss.
7. Mantovani 2019, p. 1447 ss.
8. Thiene 2021, p. 240 ss.
9. Finocchiaro 2008, p. 207 ss., spec. p. 213.
10. Senigaglia 2023, p. 470 ss., spec. p. 476. Cfr. Cacace 2025, p. 333 ss.; Foglia 2018.

soggetti che eseguono il trattamento e della loro funzione[11]. Partendo da tale constatazione, si coglie come proprio questo ambito sperimenti la tensione fra i valori e richieda un bilanciamento attento[12]. Là dove, infatti, si consideri la peculiare sensibilità delle informazioni, emerge la necessità di una più elevata difesa della persona, mentre, considerando l'interesse pubblico perseguito, si evince l'esigenza del limite al diritto individuale[13]: linee di tutela che sembrano muoversi in direzioni opposte.

2. Trattamento dei dati personali in ambito sanitario e trattamento dei dati relativi alla salute

La tutela della persona rispetto alla circolazione delle informazioni che la riguardano è stata affidata, in origine, al consenso dell'interessato. Il consenso era visto come lo strumento per mezzo del quale il soggetto poteva esercitare un controllo sul fenomeno circolatorio dei dati, nel suo duplice senso: in positivo, quando prestato, legittimando il trattamento dei dati personali e permettendo al titolare del trattamento di svolgere le relative operazioni; e in negativo, quando non prestato, rendendo illecito il trattamento che fosse comunque avvenuto e che non trovasse altra base giuridica e quindi attivando il meccanismo sanzionatorio[14].

La Direttiva UE n. 46 del 1995, che contemplava il consenso dell'interessato quale base giuridica del trattamento di dati personali al menzionato art. 7, lett. *a*, lasciava agli Stati membri il consueto margine di discrezionalità nell'attuare anche questa previsione, come disposto all'art. 5. La scelta del legislatore italiano fu quella di attribuire al consenso una funzione di perno della disciplina della protezione dei dati personali, attorno al quale far ruotare l'esercizio dei diritti dell'interessato.

Il panorama è mutato con l'entrata in vigore del GDPR[15]. Il consenso dell'interessato è solo una delle differenti condizioni di liceità del trattamento, ai sensi dell'art. 6 GDPR, e – qualificato come "esplicito" – è solo una delle ipotesi di deroga al divieto di trattamento delle categorie particolari di dati personali, ai sensi dell'art. 9 GDPR[16]. La novità non è tanto nel contenuto di queste disposizioni quanto nella tipologia di atto normativo adottato. Se la Direttiva, dovendo essere attuata, presupponeva la mediazione dell'intervento del legislatore nazionale, il Regolamento, invece, è direttamente applicabile e – pur se non elimina del tutto il margine di discrezionalità lasciato agli Stati membri, soprattutto alla luce di molteplici formulazioni normative volutamente ampie, che a loro volta richiedono un'attuazione da parte degli ordinamenti nazionali – trasferisce la sua impostazione nei sistemi giuridici europei in modo immediato.

Il discorso assume uno spessore maggiore se si considera che il trattamento di dati personali in ambito sanitario è forse quello che maggiormente ha ad oggetto i dati relativi alla salute. Com'è noto questa tipologia di dati personali rientra nel novero delle particolari categorie di dati personali per le quali si prevedono misure più rigorose in ordine al loro trattamento. Si tratta di quelle informazioni che tradizionalmente rientrano nel concetto di "dati sensibili" e il cui trattamento è in grado di mettere a serio rischio le libertà e diritti fondamentali della persona[17].

Come anticipato, l'art. 9, par. 1, GDPR vieta il trattamento di dati relativi alla salute, ma, al

11. Sandulli 2023, p. 1 ss. Cfr., per le linee di sviluppo del diritto sanitario, Sandulli–Aperio Bella 2021.
12. Evidenzia la centralità del rapporto fra privacy e attività della pubblica amministrazione P. Perlingieri 2003, p. 211 ss. Sul valore della persona e il principio personalista nel sistema ordinamentale italiano, nel rispetto del quale necessariamente deve compiersi ogni bilanciamento, v. P. Perlingieri 2020, vol. III, p. 1 ss.; nonché P. Perlingieri 1972.
13. C. Perlingieri 2022, p. 127 ss. Cfr. Di Ciommo 2002, p. 121 ss.
14. Cfr. Bygrave 2002, p. 150 e 154. Nel contesto italiano, *ex plurimis*, Iamiceli 2024, p. 76 ss., nonché Sica 2001, p. 621 ss.; Patti 1999, p. 455 ss.; Cuffaro 1997, p. 201 ss.
15. Cfr. P. Perlingieri 2018, p. 481 ss.
16. Thiene 2023, p. 7 ss.; Granieri 2017, p. 165 ss. Cfr. Georgieva–Kuner 2020, p. 365 ss.
17. Thiene–Corso 2023; Guarda 2019, p. 591 ss.; Riccio 2004, p. 247 ss.; Zambrano 1999, p. 1 ss.

contempo, il rigore del divieto è mitigato dall'elenco delle ipotesi eccezionali in cui tale trattamento è ammesso secondo il par. 2 dello stesso articolo. È proprio attraverso queste fattispecie derogatorie che il trattamento di dati sensibili, in ambito sanitario, è consentito. Oltre alle ipotesi riconducibili alla volontà della persona, ossia le eccezioni di cui alle lett. *a* ed *e* – cioè il consenso esplicito dell'interessato e la pubblicazione manifesta dei dati stessi da parte dell'interessato – giocano un ruolo di fondamentale importanza a tal fine le ipotesi enunciate alle lett. *c*, *g*, *h*, *i* e *j*.

Prima fra tutte, l'eccezione di cui alla lett. *h*, che si sostanzia nella c.d. "finalità di cura", permette il trattamento dei dati relativi alla salute, qualora necessario, per l'erogazione dei servizi e delle prestazioni di natura medica e sanitaria, non solo sulla base del diritto eurounitario o nazionale, ma anche "conformemente al contratto con un professionista della sanità". Viene così coperto il panorama del settore pubblico tanto quanto quello del settore privato. La disposizione è integrata dalla previsione dell'art. 9, par. 3, secondo cui il trattamento per finalità di cura di dati sanitari, oltre alle altre categorie particolari di dati personali, deve avvenire soltanto ad opera o sotto la responsabilità di un professionista vincolato al segreto professionale o di un soggetto comunque tenuto all'obbligo di segretezza. Va considerato che il trattamento di dati relativi alla salute in ambito sanitario è parte essenziale del rapporto medico-paziente ed è indispensabile per l'individuazione e l'esecuzione del trattamento sanitario e per lo svolgimento della funzione di un sistema sanitario[18].

Il trattamento di dati relativi alla salute in ambito sanitario è permesso, sotto altri aspetti, anche dalle altre ipotesi menzionate[19]. Così, con l'applicazione della lett. *c*, si consente il trattamento di dati sanitari che risulti necessario per un trattamento sanitario salvavita o richiesto in condizioni gravi di salute. Per la ricerca in ambito medico, la lett. *j* permette il necessario trattamento dei dati sulla salute. Mentre su un più generale versante amministrativo si colloca l'applicabilità delle eccezioni enunciate alle lett. *g* ed *i*. Se quest'ultima, infatti, viene in rilievo per i trattamenti di dati sanitari necessari per motivi pubblici legati alla sanità pubblica, quindi anche per garantire il buon funzionamento dei sistemi sanitari stessi, la lett. *g* si apre alle esigenze più ampie, non solo quelle che si prospettano come strettamente connesse alla sanità pubblica, ma anche le esigenze delle pubbliche amministrazioni, purché il trattamento di dati relativi alla salute sia necessario per "motivi di interesse pubblico rilevante".

L'importanza del trattamento dei dati sanitari – e delle altre tipologie di dati sensibili – a scopi legati alla tutela della salute è sottolineata anche dal considerando 53 del Regolamento, per cui "le categorie particolari di dati personali che meritano una maggiore protezione dovrebbero essere trattate soltanto per finalità connesse alla salute, ove necessario per conseguire tali finalità a beneficio delle persone e dell'intera società, in particolare nel contesto della gestione dei servizi e sistemi di assistenza sanitaria o sociale, compreso il trattamento di tali dati da parte della dirigenza e delle autorità sanitarie nazionali centrali a fini di controllo della qualità, informazione sulla gestione e supervisione nazionale e locale generale del sistema di assistenza sanitaria o sociale, nonché per garantire la continuità dell'assistenza sanitaria o sociale e dell'assistenza sanitaria transfrontaliera o per finalità di sicurezza sanitaria, controllo e allerta o a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in base al diritto dell'Unione o nazionale che deve perseguire un obiettivo di interesse pubblico, nonché per studi svolti nel pubblico interesse nell'ambito della sanità pubblica".

Peraltro il settore sanitario non è l'unico in cui avviene il trattamento di dati relativi alla salute. Esso, infatti, si svolge in numerosi ambiti, anche per scopi più strettamente legati al mondo dell'economia. Anche per questo l'esigenza di delineare attentamente le eccezioni al divieto di trattamento si impone con forza, soprattutto nella rapida

18. "L'informazione è dunque al centro delle organizzazioni sanitarie forse anche più della conoscenza. Le informazioni sanitarie sono cresciute in numero e complessità e sono divenute forse la prima preoccupazione delle strutture sanitarie", Comandé 2008, p. 289.

19. Cfr. Greco 2019, p. 244 ss., spec. p. 249 ss.

evoluzione tecnologica che contraddistingue la società contemporanea[20].

Il GDPR rinuncia a una completa uniformazione delle discipline nazionali, lasciando alla discrezionalità degli Stati membri la possibilità di condizionare e anche limitare il trattamento dei dati relativi alla salute, così come quello dei dati genetici e biometrici, attraverso il mantenimento delle normative interne o l'introduzione di nuove regole, per certi versi seguendo una logica simile a quella armonizzante della direttiva: la disposizione di riferimento in questo caso è il par. 4 dell'art. 9[21].

Numerose altre regole dettate dal GDPR possono trovare applicazione con riguardo al trattamento dei dati personali in ambito sanitario, ma il ruolo principale è giocato proprio dall'art. 9, che definisce così uno statuto generale per i dati sensibili e quindi include le norme di base del trattamento dei dati relativi alla salute. La disciplina del trattamento di dati personali in ambito sanitario tuttavia non si esaurisce nel Regolamento generale sulla protezione dei dati, nonostante questo rimanga il più rilevante atto normativo di riferimento. Una parte delle norme in materia è al di fuori del diritto eurounitario e ricade nel diritto interno. Così, nell'ordinamento italiano, assumono rilievo al riguardo le disposizioni del Codice della privacy.

3. Le norme del Codice della privacy

Per adeguare l'assetto del proprio sistema all'avvento del GDPR, il legislatore italiano è intervenuto sul Codice della privacy apportando numerose ed estese modifiche mediante il d.lgs. 10 agosto 2018, n. 101[22]. Si è quindi inciso profondamente sulla struttura e sul testo delle disposizioni del Codice della privacy, abrogando interi blocchi di articoli, sostituendone e modificandone altri, introducendone di nuovi, con una tecnica legislativa che non è andata esente da critiche[23].

L'abrogazione dell'art. 4 ha comportato l'eliminazione della definizione di *dati sensibili*, contenuta alla lett. *d*, essendo ora assorbita dalla valenza dell'espressione "categorie particolari di dati personali" di cui all'art. 9 del GDPR. Il Titolo III della Parte I del d.lgs. n. 196 del 2003 è stato abrogato per intero, con tutti gli articoli che conteneva, compresi gli artt. 20 e 26 applicabili appunto ai dati sensibili. Una parte assai rilevante delle nuove disposizioni, introdotte nel 2018, si trova agli artt. 2-*bis* ss., distribuiti ora, nel Titolo I, "Principi e disposizioni generali", della Parte I. Fra questi, un ruolo di estrema importanza per il trattamento di dati personali appartenenti alle particolari categorie, anche e soprattutto per il trattamento dei dati relativi alla salute, è svolto dagli artt. 2-*sexies* e 2-*septies*[24].

L'art. 2-*sexies* precisa le condizioni di ammissibilità dei trattamenti necessari per motivi di interesse pubblico rilevante ai sensi dell'art. 9, par. 2, lett. *g*, del GDPR[25]. Essi sono ammessi, ai sensi del comma 1, "qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato"[26]. Tale disposizione è stata modificata

20. Richiamando il *mosaic of policies* di Westin 1976, p. 269, come necessità per gestire le problematiche sollevate dal trattamento di dati sanitari, Comandé 2008, p. 285, individua alcune aree in cui i dati sulla salute sono sempre maggiormente raccolti, usati e condivisi: "1. l'erogazione di servizi sanitari; 2. il pagamento delle prestazioni; 3. gli usi sociali dei dati sanitari per prevenire la diffusione di epidemie".
21. Cfr. Fares 2021, p. 23.
22. In argomento Pizzetti 2021, p. 3 ss.; Tosi 2019, p. 16 ss. Sullo spirito del Codice della privacy italiano, a seguito dell'avvento del GDPR, v. Alpa 2021, p. 995 ss.
23. Cuffaro 2018, p. 1181 ss., spec. p. 1183 s.
24. C. Perlingieri 2022, p. 130 s.
25. Cortese 2021, p. 1044 ss.
26. Il comma 2 dell'art. 2-*sexies* fornisce invece un elenco di materie in cui è considerato rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri. Tra le numerosissime ipotesi di questo elenco, si evidenziano, per la stretta connessione con i dati sanitari, quelle di cui alle lett. *t*, *u*, *v*, *z*, *aa* e *cc*.

dall'art. 9, comma 1, lett. *b*, n. 1, d.l. 8 ottobre 2021, n. 139[27] – c.d. "Decreto capienze" – convertito con modificazioni dalla legge 3 dicembre 2021, n. 205, che ha eliminato la fonte regolamentare della previsione come ipotesi di ammissibilità dei trattamenti nell'ordinamento interno e ha aggiunto invece quella degli atti amministrativi generali[28]. Il comma 1-*bis* dell'art. 2-*sexies* del Codice della privacy, introdotto dalla medesima lett. *b* dell'art. 9, comma 1, d.l. n. 139/2021, al n. 2, così come modificato dalla citata legge di conversione n. 205/2021, e specificamente dedicato al trattamento di dati relativi alla salute, è stato in seguito sostituito dall'art. 44, comma 1, del d.l. 2 marzo 2024, n. 19, convertito con modificazioni dalla legge 29 aprile 2024, n. 56, il quale ha anche aggiunto all'art. 2-*sexies* un comma 1-*ter*. Queste nuove disposizioni individuano una serie di soggetti istituzionali che, nel rispetto delle proprie finalità, possono trattare i dati personali relativi alla salute, anche mediante interconnessione. Per poter essere trattati, i dati personali dovranno essere pseudonimizzati[29]. Si può notare, sin da subito, nel trattamento dei dati relativi alla salute, la centralità del fascicolo sanitario elettronico.

L'art. 2-*septies*, invece, si pone in attuazione del par. 4 dell'art. 9 del GDPR, prevedendo, come condizione per ammettere il trattamento di dati relativi alla salute, genetici e biometrici, la conformità alle *misure di garanzia* disposte dal Garante[30]. Un particolare rilievo ricopre il comma 5, per cui le misure di garanzia sono adottate in relazione a ciascuna categoria di dati personali di cui al comma 1, ossia dati relativi alla salute, dati genetici e dati biometrici, avendo riguardo alle specifiche finalità del trattamento. In tal senso, le misure di garanzia vengono ad essere l'elemento chiave, per coniugare la limitata circolazione dei dati appartenenti alle categorie particolari e la sicurezza nel trattamento, nell'ottica del rispetto dei diritti dell'interessato.

Espressamente dedicato al trattamento di dati personali in ambito sanitario è il Titolo V della Parte II del Codice della privacy, rubricato proprio in questi termini[31]. L'intervento di adeguamento al GDPR operato con il d.lgs. n. 101/2018 ha toccato, eccezion fatta per l'art. 93, tutte le disposizioni del Titolo V[32]. L'art. 75, d.lgs. n. 196 del 2003, ora recita: "Il trattamento dei dati personali effettuato per finalità di tutela della salute e incolumità fisica dell'interessato o di terzi o della collettività deve essere effettuato ai sensi dell'articolo 9, paragrafi 2, lettere h) ed i), e 3 del regolamento, dell'articolo 2-*septies* del presente codice, nonché nel rispetto delle specifiche disposizioni di settore". La nuova disposizione, nel sottinteso riferimento all'oggetto del trattamento costituito dai dati sensibili, fa rinvio ad altre norme, prime fra tutte quelle di cui all'art. 9 del GDPR, soppiantando la precedente disposizione[33]. Ad essere richiamate sono quindi le eccezioni previste dal par. 2 dell'art. 9 che si traducono nella finalità di cura (lett. *h*) – con l'ulteriore precisazione normativa di cui al par. 3 – e nei motivi di interesse pubblico nel settore della sanità pubblica (lett. *i*).

Il trattamento di dati relativi alla salute – ma anche di dati personali appartenenti ad altre categorie particolari – quando avvenga per gli scopi menzionati, ricorrendo le necessità che sono alla base di dette deroghe, dunque prescinde dal consenso dell'interessato. Deve inoltre essere conforme alle misure di garanzia, *ex* art. 2-*septies*, e rispettare le "specifiche disposizioni di settore". Con tale formula l'art. 75 fa rinvio ad altre norme, anche di livello non primario, tracciate sempre con riguardo al trattamento di dati personali per finalità di tutela della salute. In questo caso, il

27. Per una prima analisi della norma, antecedente alle modifiche apportate dalla legge di conversione, v. Francario 2021.
28. Riportando il chiarimento del Garante, di cui alla nota del 27 novembre 2018, Cortese 2021, p. 1046, evidenzia come anche la prospettiva antecedente alle modifiche citate potesse aprire alla fonte di tipo amministrativo.
29. Si v. l'art. 4, n. 5), del GDPR.
30. Zanovello 2023, p. 129 ss., spec. 150 ss.; Zanovello 2021, p. 1051 ss.
31. Su questo assetto normativo, Riccio 2004, p. 247 ss. Cfr. Caggia 2007, p. 405 ss.
32. Molti degli articoli che componevano questo titolo sono stati abrogati: artt. 76, 81, 83, 84, 85, 86, 87, 88, 89, 90, 91 e 94.
33. Poletti 2007, p. 1195 ss.

riferimento può essere, ad esempio, alla disciplina del trattamento dei dati operato mediante il fascicolo sanitario elettronico. Per certi versi, l'art. 75 riveste un carattere programmatico, là dove, non menzionando il consenso, intende dare segno di un suo formale superamento, almeno nell'area del trattamento dei dati in ambito sanitario[34].

Il contenuto delle disposizioni "superstiti" del Titolo V, preannunciato dall'art. 77 del Codice della privacy, è costituito dalle modalità particolari per informare l'interessato e trattare i suoi dati. Dinanzi alla mutata prospettiva nei confronti del consenso, acquista un ruolo più pregnante l'informazione al paziente.

Posto che gli elementi dell'informativa sono quelli dettati agli artt. 13 e 14 del GDPR[35], l'art. 78 dispone che il medico di medicina generale, così come il pediatra di libera scelta, informi l'interessato relativamente al trattamento dei dati personali, in forma chiara e tale da rendere agevolmente comprensibili detti elementi, conformemente al principio di trasparenza[36]. La tutela dell'interessato paziente è affidata a precetti che mirano a garantire un raggiungimento di consapevolezza in ordine al trattamento dei dati che lo riguardano, specialmente quando il trattamento avvenga con gli strumenti informatici, come oggi accade maggiormente. Le modalità descritte sono estese, dall'art. 79, alle strutture che erogano prestazioni sanitarie e socio-sanitarie, le quali, sulla base di adeguate misure organizzative, possono avvalersene "in modo omogeneo e coordinato in riferimento all'insieme dei trattamenti di dati personali effettuati nel complesso delle strutture facenti capo alle aziende sanitarie" per più trattamenti di dati.

L'informazione al paziente sul trattamento dei suoi dati personali deve precedere la prestazione medica, eccezion fatta per i casi di emergenza e tutela della salute e dell'incolumità fisica enunciati all'art. 82. La regola contribuisce a confermare che nella prestazione sanitaria il trattamento dei dati relativi alla salute costituisce momento funzionale, per non dire coessenziale, alla sua esecuzione[37].

4. L'amministrativizzazione della protezione dei dati

Sin dalle prime riflessioni sulla protezione dei dati personali si è colta l'inconsistenza del consenso dell'interessato al trattamento come dispositivo di controllo nella circolazione dei dati[38]. È un'inappropriatezza che si riscontra su più fronti, se rapportata alle condizioni normali di un individuo, un utente medio dei servizi digitali.

Il più delle volte, infatti, il consenso è prestato senza alcuna consapevolezza, con disattenzione. La possibilità o la necessità di accedere velocemente a un servizio e le caratteristiche dell'ambiente digitale, alla portata di tutti, in qualsiasi luogo e in qualsiasi momento, su un computer, uno smartphone, un tablet, influiscono sui soggetti inibendo

34. Ogni riferimento al consenso è stato espunto dalle disposizioni di questo Titolo, "per effetto della mutata *ratio* normativa", Di Masi 2021, p. 1237.

35. Per la violazione degli obblighi informativi sanciti dal Regolamento e dal Codice della privacy, si è sostenuta in dottrina la configurabilità di una responsabilità contrattuale, in quanto si tratterebbe dell'inadempimento di obbligazioni derivanti *ex lege*, Piraino 2017, p. 389 s.

36. Vanno evidenziati, da parte sua, "analiticamente eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato". E ciò, in particolare, nel caso di trattamenti effettuati: "a) per fini di ricerca scientifica anche nell'ambito di sperimentazioni cliniche, in conformità alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente; b) nell'ambito della teleassistenza o telemedicina; c) per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica; c-bis) ai fini dell'implementazione del *fascicolo sanitario elettronico* di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221; c-ter) ai fini dei sistemi di sorveglianza e dei registri di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221".

37. Cfr. Finocchiaro 2008, p. 213 ss. Con riguardo, invece, al trattamento effettuato per la prescrizione di medicinali, l'art. 89 *bis* dispone che si adottino "cautele particolari" in relazione alle misure di garanzia del Garante, anche al di là della finalità di cura.

38. Cfr. Mirabelli 1993, p. 313 ss.

la considerazione che possono avere del valore della privacy e dei loro dati personali. Se l'interessato cercasse di comprendere ciò cui sta acconsentendo, spesso non sarebbe in grado di capirlo. La complicatezza delle operazioni di trattamento e la complessità tecnologica degli strumenti stessi pregiudicano l'intelligibilità delle attività e delle procedure messe in atto, la quale può richiedere conoscenze tecniche elevate e anche molto settoriali. Talvolta è l'informazione offerta all'interessato ad essere pregiudicata da questa complessità, di conseguenza ostacolando la comprensione del trattamento per cui si richiede il consenso, talaltra è anche solo il modo in cui l'informazione è resa che impedisce di comprendere. E, ancora, qualora tale consapevolezza vi fosse, la scelta sarebbe vincolata, poiché altrimenti il servizio correlato al trattamento potrebbe non essere erogato. In tal caso l'interessato avrebbe sì contezza delle operazioni di trattamento dei suoi dati personali e dei rischi connessi, ma acconsentirebbe ugualmente, per mancanza di alternative o per il bisogno di quel bene o di quel servizio[39].

Il pensiero giuridico si è, dunque, indirizzato verso altri strumenti, diversi dal consenso, per garantire la protezione dei dati personali – specie quelli sensibili – e, con essa, la protezione della persona. Le riflessioni sono approdate così ad una serie di misure e accorgimenti, soprattutto di natura tecnica, in grado di intervenire preventivamente rispetto alla possibile violazione di dati personali. E questi si sono poi tradotti in principi e regole, che possono, in larga parte, ricondursi al concetto di "sicurezza".

Così può intendersi la riservatezza per progettazione e per impostazione, cioè le nozioni di *privacy by design* e *privacy by default*[40]. Tali concetti impongono al sistema informatico di conformarsi alla protezione dei dati, sin dall'origine. L'ambiente digitale viene pensato sin dalla sua costruzione come un insieme di strutture atte a garantire la protezione dei dati personali e l'architettura dello spazio elettronico deve rispondere a questa logica[41]. In tal senso, la privacy non è più vista come un diritto corrispondente a mere pretese esercitabili dal singolo, bensì come un diritto che esige una tutela complessiva in quel contesto e da quel contesto e che quindi partecipa all'edificazione dell'ambiente digitale. Se il codice – informatico – diventa la nuova legge[42], allora il diritto modella questo codice affinché assicuri l'osservanza dei principi e delle regole, che al di fuori dello spazio elettronico è assicurata dalla legge[43].

Così può intendersi anche la tecnica della pseudonimizzazione, con cui viene impedita l'attribuzione del dato personale al soggetto cui si riferisce. L'impedimento non è irreversibile ed è sempre possibile restituire al dato pseudonimizzato la sua attribuibilità mediante l'utilizzo della specifica "chiave". In ciò la pseudonimizzazione si distingue dall'anonimizzazione, che invece spoglia irreversibilmente il dato personale della possibilità di essere attribuito alla persona e lo rende, appunto, dato anonimo[44]. La prima delle misure tecniche e organizzative che il GDPR, all'art. 32, prevede possa essere messa in atto da parte del titolare e del responsabile del trattamento per garantire un livello di sicurezza adeguato al rischio è proprio la pseudonimizzazione. Il dato pseudonimizzato è ancora dato personale e ne conserva il valore, perché l'individuo rimane identificabile, ma il trattamento che si svolge diviene più sicuro[45].

Allo stesso modo si possono intendere le procedure di valutazione del rischio[46]. Nelle

39. Cfr. Gatt–Caggiano–Montanari 2021.
40. Si v. l'art. 25 GDPR, rubricato "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita".
41. Bravo 2022, p. 85 ss.; Bravo 2019, p. 775 ss. V. anche Calzolaio 2017.
42. Secondo la celebre formula *code is law*, Lessig 1999.
43. Maestri 2015, *passim*.
44. Irti 2022, p. 49 ss.
45. Pellecchia 2020, p. 360 ss., spec. p. 362.
46. Mantelero 2019, p. 473 ss.; Mantelero 2017, p. 287 ss. Cfr. Gruppo Articolo 29, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*, 4 ottobre 2017, WP 248 rev.01.

formulazioni del GDPR, la "valutazione dei rischi per i diritti e le libertà degli interessati" è inclusa nella "valutazione d'impatto sulla protezione dei dati", ai sensi dell'art. 35, par. 7, lett. c. Al titolare del trattamento è richiesta la valutazione d'impatto quando il tipo di trattamento da effettuare può presentare un rischio elevato per i diritti e le libertà degli interessati. La procedura contempla il coinvolgimento dell'autorità di controllo, ai sensi dell'art. 36 del GDPR: se la valutazione d'impatto sulla protezione dei dati indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare per attenuare il rischio, questi deve procedere con una consultazione preventiva dell'autorità. Peraltro, il par. 5 dell'art. 36 permette agli Stati membri di prescrivere che i titolari consultino l'autorità di controllo e ne ottengano l'autorizzazione preliminare, in relazione al corrispondente trattamento per l'esecuzione di un compito di interesse pubblico, come "il trattamento con riguardo alla protezione sociale e alla sanità pubblica2.

Ma soprattutto la funzione di garanzia in ottica preventiva è assegnata al principio di *accountability*, la responsabilizzazione dei soggetti che operano il trattamento dei dati[47]. In virtù di questo principio, ai sensi dell'art. 5, par. 2, del GDPR, il titolare del trattamento è competente per il rispetto di tutti i principi del trattamento dei dati personali, *ex* art. 5, par. 1, ed è in grado di comprovarlo. Nell'ipotesi in cui il trattamento si basi sul consenso dell'interessato, il GDPR, all'art. 7, par. 1, prescrive specificamente – come declinazione della più generale responsabilizzazione del titolare – che questi debba poter dimostrare che il consenso è stato prestato. Ai sensi dell'art. 24, il titolare del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, deve adottare le misure tecniche e organizzative che non solo ne garantiscano la conformità al GDPR, ma anche gli consentano di dimostrarla.

Il principio di *accountability* "costituisce il nucleo della riforma europea e realizza un nuovo sistema normativo nel trattamento dei dati personali e nella protezione dei diritti della persona"[48]. Mediante questo principio la tutela della persona, nell'ambito della protezione dei dati personali, si può trasferire dal piano rimediale successivo e della sanzione e dal piano singolare e puntiforme del consenso dell'interessato a quello più generale e preventivo della gestione del rischio. E così acquista nuova centralità la posizione del titolare del trattamento[49]: infatti, egli deve mettere in atto misure appropriate ed efficaci per assicurare la protezione dei dati, in conformità ai principi del GDPR, e deve documentare l'adozione di queste misure, per poter rispondere a una richiesta di dimostrazione[50]. Lungi dal restare una norma meramente programmatica, il principio di *accountability* ha notevoli ricadute pratiche e organizzative, in termini operativi, per le misure concretamente da prendere, e in termini precauzionali, come precostituzione della prova. Quindi vi è un obbligo di sicurezza, gravante sui soggetti che operano il trattamento, titolare e responsabile[51].

47. Camardi 2022, p. 25 ss.; Stanzione 2022, p. 1 ss.; Amram 2020; Finocchiaro 2019, p. 2778 ss. Cfr. Gruppo Articolo 29, *Parere 3/2010 sul principio di responsabilità*, 13 luglio 2010, WP 173.

48. Così Finocchiaro 2019, p. 2778; Finocchiaro 2012, p. 289 ss.

49. Cfr. Messinetti 2019, p. 146: "al ridimensionamento della volontà del titolare dei dati personali fa da contrappunto il rafforzamento di un potere del titolare del trattamento: il diritto – appunto – di trattare i dati personali altrui".

50. Sono i due elementi di cui si compone il principio di *accountability*. V. Gruppo Articolo 29, *Parere 3/2010 sul principio di responsabilità*, cit., 9.

51. In argomento Farace 2019, p. 731 ss. V. anche Sirgiovanni 2020, p. 1013: "In altri termini, la tutela del diritto alla protezione dei dati personali sta non tanto nel negare il consenso al trattamento – in quanto spesso negare il consenso significa non ottenere il servizio – ma piuttosto nel predisporre da parte del titolare del trattamento tutte le misure idonee perché il trattamento del dato sia eseguito nel rispetto dei principi di liceità, correttezza e trasparenza del trattamento, limitando il trattamento alla specifica finalità indicata". Nella prospettiva della legge n. 675 del 1996, Bozzi 1997, p. 97 ss., affronta i profili legati ai soggetti del trattamento, mentre Conte 1997, p. 225 ss., spec. p. 262 ss., mette in relazione gli obblighi di sicurezza con i diritti dei soggetti interessati.

Una buona parte dei trattamenti di dati personali effettuati ha luogo per le attività della pubblica amministrazione e ciò vale in particolar modo per i dati relativi alla salute, considerando che uno dei settori più importanti, forse il principale, in cui essi vengono trattati è proprio quello sanitario. E, se si parla di soggetti pubblici, allora, il campo delle regole non è più – o almeno non è più soltanto – quello del diritto privato, ma è quello del diritto pubblico o, forse, meglio, del diritto amministrativo. Come è stato messo in luce in dottrina, è possibile individuare una funzione amministrativa di protezione dei dati personali, alla quale rispondono le regole volte a disciplinare la pubblica amministrazione e la sua attività là dove vengano in gioco trattamenti di dati[52].

La norma di diritto pubblico che si cala nel contesto della sanità, nella garanzia del diritto alla salute, deve dunque includere la protezione dei dati personali e, specialmente, di quelli sanitari. Come espresso proprio dalla legge Gelli-Bianco, in apertura, all'art. 1, tutte le attività finalizzate alla prevenzione e alla gestione del rischio connesso all'erogazione di prestazioni sanitarie e l'utilizzo appropriato delle risorse strutturali, tecnologiche e organizzative contribuiscono a realizzare la sicurezza delle cure, che è parte costitutiva del diritto alla salute ed è perseguita nell'interesse dell'individuo e della collettività. Con ciò può comprendersi come nella tutela del diritto alla salute vadano ricompresi tutti quei requisiti organizzativi finalizzati a garantire trasparenza ed efficienza delle risorse e implicanti l'uso delle tecnologie[53]. La protezione dei dati personali partecipa quindi del diritto alla salute, come diritto della personalità e nell'orizzonte unitario – concettuale, giuridico – della persona umana.

Perciò si fa preminente la regolazione amministrativistica su quella privatistica. Questo superamento è l'*amministrativizzazione della protezione dei dati personali*[54]. Il fatto che le disposizioni non siano più – o non più tanto – di diritto privato, ma di diritto amministrativo non cambia il modo in cui vadano interpretate, alla luce del principio personalista e della dignità, che irradia l'ordinamento tutto.

5. Il fascicolo sanitario elettronico

Con lo sviluppo della sanità digitale si assiste a un aumento delle attività di trattamento di dati personali in ambito sanitario e quindi di dati relativi alla salute, mediante strumenti tecnologici e informatici. L'incremento delle operazioni di trattamento conferisce importanza maggiore alla normativa in materia di protezione dei dati sanitari.

Da questo punto di vista un plesso normativo in particolare assume grande rilevanza nell'ordinamento italiano, per il carattere applicativo e al contempo sistematico delle sue disposizioni rispetto alla materia della protezione dei dati personali, e cioè la disciplina del fascicolo sanitario elettronico (c.d. FSE)[55]. Si tratta peraltro di una disciplina in costante mutamento, mai assestatasi definitivamente, e anzi oggi in fase di rapidi aggiustamenti, per restare al passo con l'incessante innovazione tecnologica e con l'evoluzione del quadro normativo, specialmente su impulso del diritto eurounitario.

L'art. 12 del d.l. 18 ottobre 2012, n. 179, con cui il FSE fu formalmente istituito, è stato modificato dal legislatore finora per ben undici volte[56]. Le

52. Bombardelli 2022, p. 351 ss. V. anche Franca 2023. Cfr. Carullo 2018.

53. Amram–Comandé 2018, p. 1 ss. Cfr. Alpa 2022, p. 89 ss.

54. Corso 2024, p. 334 ss.; Corso 2023, p. 91 ss. Una amministrativizzazione della protezione dei dati si può osservare anche nel maggior peso dato all'atto amministrativo come fonte del diritto. A tal proposito, si considerino anche le modifiche apportate all'art. 2-*ter* del Codice della privacy ad opera del d.l. n. 139/2021, Francario 2021. Cfr. Francario 2022, p. 679 ss.

55. Sul FSE, senza pretesa di esaustività, v. Capilli 2025, p. 7 ss.; Catelani 2023, p. 423 ss.; Posteraro–Corso 2023, p. 187 ss.; Silvano 2023, p. 228 ss.; Posteraro 2022, p. 187 ss.; Posteraro 2021; Pioggia 2021, p. 215 ss.; Gambino–Maggio–Occorsio 2020; Bottari 2017, p. 65 ss.; Comandé–Nocco–Peigné 2012, p. 105 ss.; Finocchiaro 2012; Guarda 2011; Peigné 2011, p. 1519 ss. V. anche Corso 2020, p. 393 ss.

56. Dopo le modifiche dettate dall'art. 1, comma 1, l. 17 dicembre 2012, n. 221, in sede di conversione, l'articolo è stato ritoccato dall'art. 17, comma 1, lett. a, d.l. 21 giugno 2013, n. 69, convertito, con modificazioni, dalla l. 9 agosto 2013 n. 98. A queste hanno fatto seguito quelle di cui all'art. 1, l. 11 dicembre 2016, n. 232; art. 1, comma 558,

regole dettate dall'art. 12 sono completate da una normativa più dettagliata affidata a più decreti, principalmente del Ministero della salute. Il primo "regolamento" in materia di FSE, infatti, fu dettato dal d.p.c.m. n. 178 del 2015. Le disposizioni ivi contenute sono state poi abrogate dai decreti del Ministero della salute 7 settembre 2023, c.d. "decreto FSE 2.0", e 31 dicembre 2024, il decreto istitutivo dell'ecosistema dati sanitari (c.d. EDS). Nel frattempo, il decreto FSE 2.0 è stato già oggetto di modifiche ad opera del decreto del Ministero della salute 30 dicembre 2024.

Il FSE è un "contenitore" di dati personali e, come tale, di dati personali è alimentato. Ad alimentarlo sono i dati degli eventi clinici presenti e trascorsi riguardanti l'assistito, inerenti anche alle prestazioni erogate al di fuori del Servizio sanitario nazionale, in maniera continuativa e tempestiva dai soggetti e dagli esercenti le professioni sanitarie che hanno in cura l'assistito stesso nonché, su iniziativa di quest'ultimo, con i dati medici in suo possesso[57].

Da un esame complessivo delle disposizioni in materia, si evince come l'impiego del FSE consenta di raggiungere plurime finalità. La finalità di cura e assistenziale è solo una di queste, che si aggiunge alla finalità di ricerca e a varie finalità di carattere pubblico. Per il conseguimento degli obiettivi corrispondenti a queste varie finalità ora al FSE si affianca l'EDS, una banca dati in cui confluiscono le informazioni comprese nel FSE, che possono quindi essere gestite separatamente, soprattutto per gli scopi di carattere pubblico. All'assistito sono riconosciuti vari "diritti" ed è attraverso questi che egli vede garantita la propria autodeterminazione. Si pensi al diritto di accesso, che gli consente di avere contezza dei dati e dei documenti caricati nel FSE, o il diritto all'oscuramento, che gli permette di nascondere i referti presenti nel FSE ai professionisti che vi abbiano accesso. Il consenso dell'assistito rileva ai fini della consultazione: egli cioè può acconsentire o negare l'accesso al suo FSE agli esercenti le professioni sanitarie che intendano consultarlo per finalità di diagnosi, cura e riabilitazione, prevenzione, profilassi internazionale.

Ma la disciplina del FSE è emblematica del nuovo modo di intendere il consenso proprio perché consente trattamenti di dati personali e di dati sanitari a prescindere dal consenso dell'interessato stesso. Infatti, il comma 3-*bis*[58] dell'art. 12 d.l. n. 179/2012, secondo cui "il FSE può essere alimentato esclusivamente sulla base del consenso libero e informato da parte dell'assistito, il quale può decidere se e quali dati relativi alla propria salute non devono essere inseriti nel fascicolo medesimo", è stato abrogato dal d.l. n. 34/2020[59]. La scelta di procedere all'abrogazione cancellando il requisito del consenso è in linea con le affermazioni del Garante per la protezione dei dati personali, che nel provvedimento del 7 marzo 2019, n. 55 aveva ammesso, forse un po' frettolosamente, la possibile eliminazione della necessità di acquisire il consenso dell'interessato all'alimentazione del fascicolo. La posizione del Garante si basava sul quadro normativo rinnovato, a seguito dell'entrata in vigore del Regolamento generale sulla protezione dei dati e del d.lgs. n. 101/2018, di adeguamento delle disposizioni contenute nel Codice della privacy[60].

Si può notare dunque come la previsione dell'interesse pubblico rilevante e dell'interesse pubblico nel settore della sanità pubblica, tra le eccezioni al divieto di trattamento di dati sanitari,

l. 30 dicembre 2018, n. 145; art. 3, l. 22 marzo 2019, n. 29; art. 11, d.l. 19 maggio 2020, n. 34, convertito, con modificazioni, dalla l. 17 luglio 2020, n. 77; art. 21, d.l. 27 gennaio 2022, n. 4, convertito, con modificazioni, dalla l. 28 marzo 2022 n. 25; art. 42, comma 1, lett. *a*, d.l. 2 marzo 2024, n. 19, convertito, con modificazioni, dalla l. 29 aprile 2024, n. 56; art. 36, comma 2, d.lgs. 3 maggio 2024, n. 62. Invece la l. 23 settembre 2025, n. 132, recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", all'art. 10 introduce l'art. 12-*bis* del d.l. 179/2012, per regolare aspetti dell'intelligenza artificiale nel settore sanitario.

57. V. art. 12, commi 1 e 3, d.l. n. 179/2012.

58. Introdotto dall'art. 1, comma 1, l. 17 dicembre 2012, n. 221, in sede di conversione.

59. Gambino–Maggio–Occorsio 2020. L'abrogazione, precisamente, si è avuta ad opera dell'art. 11, comma 1, lett. *d*, d.l. 19 maggio 2020, n. 34, convertito, con modificazioni, dalla l. 17 luglio 2020, n. 77. Al riguardo v. Miccú 2021, p. 11 ss.; Covino 2021, p. 66 ss.; Sorrentino–Spagnuolo 2020, p. 251.

60. Cuttaia 2021, p. 195 ss., spec. p. 200 s.; Foglia 2020, p. 43 ss. Sia concesso il rinvio a Corso 2019, p. 225 ss.

possa tradursi in una valvola di apertura, quasi una clausola generale, in grado di oltrepassare il divieto ex art. 9 par. 1 GDPR, al ricorrere del generale elemento pubblicistico. La protezione dei dati personali – e specialmente relativi alla salute – si connota, quindi, sempre più come materia di diritto pubblico e amministrativo, perdendo rilievo la connotazione privatistica che la descriveva sostanzialmente come un diritto dei singoli, come una questione di riserbo o un affare tra privati. La tutela della persona – e lo si può intendere anche dall'evoluzione del FSE – è affidata, dunque, al piano della sicurezza, che concretamente andrà garantita e implementata dai titolari del trattamento.

La garanzia dell'autodeterminazione permane – e con essa un'area di autonomia, che restituisce spazio al diritto privato – nel novero dei diritti dell'interessato e dell'assistito, pur con tutti i grossi limiti dell'attuale assetto normativo. Si pensi, ad esempio, ai limiti che incontra indistintamente il diritto alla cancellazione, sancito dall'art. 17 GDPR, là dove si tratti di trattamenti di dati necessari per motivi di interesse pubblico nel settore della sanità pubblica (par. 3, lett. c, dell'art. 17)[61]. L'assunto circa il rilievo dei diritti riconosciuti al singolo, in chiave di autodeterminazione rispetto al trattamento di dati relativi alla salute, trova riscontro nella nuova disciplina dello spazio europeo dei dati sanitari, dettata dal reg. Ue n. 327 del 2025.

6. Lo spazio europeo dei dati sanitari

Il Regolamento UE 2025/327 dell'11 febbraio 2025, pubblicato nella Gazzetta Ufficiale dell'Unione europea il 5 marzo 2025, ha istituito lo *European Health Data Space* (c.d. EHDS), lo spazio europeo dei dati sanitari. Nuova tappa del percorso del diritto della tecnologia, il Regolamento sull'EHDS rappresenta il frutto di un impegno che dura da anni per realizzare, sul piano giuridico, un ambiente digitale sicuro in cui trattare dati sanitari, essenziale per la digitalizzazione della sanità. Esso si colloca primariamente nell'ambito della strategia europea dei dati, ma al contempo rappresenta un elemento fondamentale dell'Unione europea della salute[62].

L'istituzione dell'EHDS si compie, come espresso dall'art. 1, par. 1, del reg. UE n. 327 del 2025, con la previsione di "disposizioni, norme e infrastrutture comuni e un quadro di governance al fine di facilitare l'accesso ai dati sanitari elettronici per l'uso primario dei dati sanitari elettronici e l'uso secondario di tali dati". La creazione dell'EHDS è diretta a garantire a ciascuno un accesso semplice e immediato ai propri dati sanitari in formato elettronico, un'agevole loro condivisione con i professionisti sanitari, anche in Stati membri diversi, e un controllo sui dati stessi, in una cornice di interoperabilità e sicurezza. Ha anche lo scopo di favorire un mercato unico per i sistemi di cartelle cliniche elettroniche e di delineare un quadro giuridico coerente, affidabile ed efficiente per riutilizzare i dati sanitari in ambito pubblico, come per la ricerca, l'innovazione, la determinazione delle politiche. Le finalità perseguite sono in realtà molteplici, ma possono simbolicamente raggrupparsi in due categorie, che strutturano l'intero Regolamento: l'*uso primario* e l'*uso secondario*. In estrema sintesi l'uso primario è l'utilizzo dei dati per l'assistenza sanitaria e i servizi connessi, mentre l'uso secondario è l'impiego dei dati per finalità diverse dalle finalità iniziali per cui i dati sono stati raccolti o prodotti.

Il Regolamento sull'EHDS si pone espressamente in relazione con il GDPR, a sua integrazione e specificazione, come enunciato all'art. 1. Inoltre, secondo il par. 3 dell'art. 1, esso "lascia impregiudicati gli altri atti giuridici dell'Unione relativi all'accesso ai dati sanitari elettronici, alla loro condivisione o al loro uso secondario o le prescrizioni dell'Unione relative al trattamento dei dati in relazione ai dati sanitari elettronici" e, in particolare, lascia "impregiudicato" il reg. Ue n. 679 del 2016. La disciplina dettata dal GDPR continua dunque a trovare applicazione, senza modifiche. Tuttavia, in relazione al trattamento di dati sanitari elettronici prende corpo un assetto normativo di dettaglio.

Le definizioni stesse, fornite dall'art. 2 del Regolamento sull'EHDS, poggiano, in buona parte, su quelle rese dal GDPR. Spicca, per il rilievo assunto nell'ambito dell'EHDS e in relazione alla protezione dei dati personali, la definizione di "dati sanitari elettronici personali", di cui all'art. 2, par. 2, lett. a, cioè "i dati relativi alla salute e i dati genetici che sono trattati in formato elettronico". Non

61. C. Perlingieri 2022, p. 127 ss.

62. Catanzariti 2025; Morace Pinelli 2025-a, p. 1016 ss.; Morace Pinelli 2025-b; Slokenberga–Ó Cathaoir–Shabani 2025; C. Perlingieri 2024, p. 485 ss. Sia consentito di rinviare a Corso 2025, p. 563 ss.

vi è identità quindi tra la nozione di "dati sanitari elettronici" – che possono essere anche dati non personali – e quella di "dati relativi alla salute". Il formato elettronico, che è elemento attinente alla modalità di trattamento, individua una sottocategoria di dati personali sensibili ai quali si applica la specifica disciplina del reg. Ue n. 327 del 2025. Come espresso al considerando 7, l'impiego per via elettronica di dati sanitari è comune e funzionale ai sistemi sanitari nazionali, in cui vengono raccolti tramite le cartelle cliniche elettroniche, "che solitamente contengono l'anamnesi di una persona fisica, diagnosi e cure, medicinali, allergie e vaccinazioni, nonché immagini radiologiche, risultati di laboratorio e altri dati medici, distribuiti tra i diversi soggetti del sistema sanitario, quali medici di base, ospedali, farmacie o servizi di assistenza". Poiché i dati sanitari elettronici personali vengono definiti come un sottoinsieme di dati relativi alla salute ed essendo questi dati personali appartenenti alle categorie particolari, valgono per il loro trattamento le regole dettate dal GDPR per i dati sensibili, ossia il divieto generale, derogato nelle ipotesi espressamente previste. Si rinfrancano così l'incisività e l'estensione dell'interesse pubblico come legittimazione del trattamento dei dati personali, espressa dagli artt. 6, par. 1, lett. e, e 9, par. 2, lett. g, del reg. Ue n. 679 del 2016, esplicitamente menzionati dal reg. Ue n. 327 del 2025.

Tra le norme più significative del Regolamento sull'EHDS vi è il riconoscimento del diritto delle persone fisiche all'*esclusione*, verso il trattamento di propri dati sanitari elettronici personali. L'EHDS contempla quindi la possibilità che gli interessati esercitino un *opt-out*, rispetto allo spazio europeo stesso. Punto di equilibrio fra le esigenze della collettività all'utilizzo dei dati sanitari e le istanze di tutela del singolo, esso rappresenta un contemperamento funzionale tanto all'uso primario quanto all'uso secondario dei dati sanitari elettronici, nel rispetto delle libertà e dei diritti fondamentali della persona. Il diritto all'esclusione consiste nel diritto a che siano impediti l'accesso ai propri dati sanitari elettronici e la loro messa a disposizione per i servizi dell'EHDS. Aggiungendosi ai diritti dell'interessato[63], esso contribuisce sensibilmente a garantire l'autodeterminazione del soggetto rispetto ai trattamenti di dati sanitari che lo riguardino, pur se non comporta una cancellazione dei dati stessi, che invece sembrano permanere all'interno dell'EHDS.

Nodale, in ordine all'uso secondario dei dati sanitari elettronici, è il ruolo svolto dall'autorizzazione ai dati, che l'organismo responsabile rilascia, ai sensi dell'art. 68, sulla base della domanda e a seguito della valutazione di una serie di requisiti. Secondo la definizione dell'art. 2, par. 2, lett. v, la "autorizzazione ai dati", è "una decisione amministrativa": è chiaro qui il senso della amministrativizzazione della protezione dei dati.

Nel complesso, le nuove disposizioni raffigurano uno scenario ancora futuro – l'applicazione del reg. Ue n. 327 del 2025, infatti, è rinviata a partire dal 2027, con differenti scaglioni per più fasi temporali – per certi versi avveniristico – in quanto si coniuga con lo sviluppo delle tecnologie più nuove, come l'intelligenza artificiale, e quelle tuttora ignote che saranno fatte proprie dalla sanità digitale – ove trova valorizzazione il bisogno superindividuale legato al trattamento dei dati sanitari, di cui si fa portatrice l'amministrazione pubblica, ma sempre con l'osservanza dei diritti del singolo. L'EHDS si connota dunque, da un lato, per il rapporto diretto e speciale con la disciplina della protezione dei dati personali e, dall'altro, per la concezione del dato sanitario come di una informazione destinata a circolare e che *dovrà* circolare, eventualmente anche a prescindere dalla posizione del soggetto cui le informazioni stesse si riferiscono. L'avvento dell'EHDS conferma la fine del consenso al trattamento dei dati personali come strumento di tutela per eccellenza del soggetto dinanzi al fenomeno circolatorio dei dati e lo fa in relazione non a una categoria qualsiasi di dati, bensì rispetto proprio ai dati che più di tutti potrebbero astrattamente pregiudicare l'individuo stesso, se trattati. Le norme del GDPR non vengono toccate, ma trovano sviluppi proprio là dove ottimizzano la circolazione dei dati per ragioni di interesse pubblico. Ciò non significa che il consenso non svolga più alcun ruolo e non significa nemmeno che la volontà del soggetto non possa valere nell'esercizio dei suoi diritti soggettivi. Anzi, attraverso le norme nuove, che arricchiscono le situazioni giuridiche del soggetto interessato, si possono cogliere nuove sfumature dell'autodeterminazione della persona.

63. Cfr. Faillace 2025, p. 379 ss. V. anche Cacace 2025, p. 333 ss.

Il quadro giuridico che si staglia così all'orizzonte, seppur comunque perfettibile, racchiude il bilanciamento fra l'interesse di carattere pubblico, all'impiego dei dati sanitari, e quello di carattere privato, in capo ai singoli, che è anche interesse dei pazienti alla cura migliore. Spetterà all'interpretazione ricondurre queste disposizioni alla coerenza del sistema, conferendo ad esse il significato più corretto nel rispetto dei principi dell'ordinamento e illuminando il percorso ancora da seguire, verso la garanzia più effettiva della dignità della persona[64].

Riferimenti bibliografici

G. Alpa (2022), *Salute e medicina*, in G. Alpa (a cura di),"La responsabilità sanitaria. Commento alla l. 8 marzo 2017, n. 24", 2ª ed., Pacini, 2022

G. Alpa (2021), *sub art. 1, d.lgs. 30 giugno 2003, n. 196*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), "Codice della privacy e *data protection*", Giuffrè, 2021

D. Amram (2020), *Building up the "Accountable Ulysses" model. The impact of GDPR and national implementations, ethics, and health-data research: Comparative remarks*, in "Computer Law & Security Review", vol. 37, 2020

D. Amram, G. Comandé (2018), *Sul non facile coordinamento degli obblighi imposti dal Regolamento europeo sulla protezione dei dati personali UE/679/2016 e dalla legge n. 24/2017*, in "Rivista italiana di medicina legale", 2018

M. Bombardelli (2022), voce *Dati personali (tutela dei)*, in "Enciclopedia del diritto. I tematici. III, Funzioni amministrative", Giuffrè, 2022

C. Bottari (2017), *L'inquadramento costituzionale del Fascicolo Sanitario Elettronico*, in "Salute e società", 2017, n. 2

L. Bozzi (1997), *I soggetti coinvolti nell'attività di trattamento*, in V. Cuffaro,V. Ricciuto (a cura di), "La disciplina del trattamento dei dati personali", Giappichelli, 1997

F. Bravo (2022), *Data Management Tools and Privacy by Design and by Default*, in R. Senigaglia, C. Irti, A. Bernes (eds.), "Privacy and Data Protection in Software Services", Springer, 2022

F. Bravo (2019), *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

L.A. Bygrave (2002), *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer Law International, 2002

S. Cacace (2025), *Autodeterminazione, paternalismo e responsabilità: l'uso primario dei dati sanitari nella relazione di cura e di fiducia fra medico e paziente*, in "Responsabilità medica", 2025

F. Caggia (2007), *Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "Il codice del trattamento dei dati personali", Giappichelli, 2007

V. Calderai (2015), voce *Consenso informato*, in "Enciclopedia del diritto, Annali VIII", 2015

64. "È indubitabile che i dati dei pazienti rappresentano una risorsa di valore inestimabile per la ricerca e per la migliore cura, ma è altrettanto palese che è necessario che vi sia un contesto, normativo e fattuale, all'interno del quale sia realmente possibile valorizzarli in tutta la loro potenzialità, salvaguardando nel contempo il rispetto dei diritti della persona. In questa prospettiva è dunque indispensabile perseguire e realizzare un corretto equilibrio tra i diversi diritti e interessi, individuando la loro possibile conciliazione non in termini astratti, ma sulla base delle esperienze concrete", Sandulli 2023, p. 4.

S. Calzolaio (2017), Privacy by design. *Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in "federalismi.it", 2017, n. 24

C. Camardi (2022), *Liability and Accountability in the 'Digital' Relationships*, in R. Senigaglia, C. Irti, A. Bernes (eds.), "Privacy and Data Protection in Software Services", Springer, 2022

G. Capilli (2025), *Diritto privato sanitario. Fondamenti*, 2ª ed., Pacini, 2025

G. Carullo (2018), *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Giappichelli, 2018

M. Catanzariti (a cura di) (2025), *Lo spazio europeo dei dati sanitari: una riflessione interdisciplinare su diritto, etica e scelte pubbliche*, in "Notizie di Politeia", 2025, n. 158

E. Catelani (2023), *La digitalizzazione dei dati sanitari: un percorso ad ostacoli*, in "Corti supreme e salute", 2023

G. Comandé (2008), *Circolazione elettronica dei dati sanitari e regolazione settoriale: spunti ricostruttivi su «interferenze sistematiche»*, in F. Ruscello (a cura di), "Studi in onore di Davide Messinetti", I, Edizioni Scientifiche Italiane, 2008

G. Comandé, L. Nocco, V. Peigné (2012), *Il fascicolo sanitario elettronico: uno studio multidisciplinare*, in "Rivista italiana di medicina legale", 2012

G. Conte (1997), *Diritti dell'interessato e obblighi di sicurezza*, in V. Cuffaro, V. Ricciuto (a cura di), "La disciplina del trattamento dei dati personali", Giappichelli, 1997

S. Corso (2025), *Lo spazio europeo dei dati sanitari. Prime riflessioni sul regolamento UE 2025/327*, in "Nuove leggi civili commentate", 2025, n. 3

S. Corso (2024), *Il fascicolo sanitario elettronico 2.0. Spunti per una lettura critica*, in "Nuove leggi civili commentate", 2024, n. 2

S. Corso (2023), *Sanità digitale e riservatezza. Interpretazioni sul fascicolo sanitario elettronico*, in A. Thiene, S. Corso (a cura di), "La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza", Jovene, 2023

S. Corso (2020), *Il fascicolo sanitario elettronico fra* e-Health, privacy *ed emergenza sanitaria*, in "Responsabilità medica", 2020

S. Corso (2019), *Sul trattamento dei dati relativi alla salute in ambito sanitario: l'intervento del Garante per la protezione dei dati personali*, in "Responsabilità medica", 2019

F. Cortese (2021), *sub art. 2 sexies, d.lgs. 30 giugno 2003, n. 196*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), "Codice della privacy e *data protection*", Giuffrè, 2021

F. Covino (2021), *Uso della tecnologia e protezione dei dati personali sulla salute tra pandemia e normalità*, in "federalismi.it", 2021, n. 5

V. Cuffaro (2018), *Quel che resta di un codice: il D.Lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al regolamento sulla protezione dei dati*, in "Corriere giuridico", 2018

V. Cuffaro (1997), *Il consenso dell'interessato*, in V. Cuffaro,V. Ricciuto (a cura di), "La disciplina del trattamento dei dati personali", Giappichelli, 1997

F.G. Cuttaia (2021), *The impact of EU Regulation 2016/679 on the Italian health system*, in G. Fares (ed.), "The Protection of Personal Data Concerning Health at the European Level. A Comparative Analysis", Giappichelli, 2021

F. Di Ciommo (2002), *Il trattamento dei dati sanitari tra interessi individuali e collettivi*, in "Danno e responsabilità", 2002

M. Di Masi (2021), *sub art. 75, d.lgs. 30 giugno 2003, n. 196*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), "Codice della privacy e *data protection*", Giuffrè, 2021

S. Faillace (2025), *I diritti dell'interessato nell'uso primario dei dati sanitari elettronici secondo il nuovo Regolamento EHDS*, in "Contratto e impresa", 2025

D. Farace (2019), *Il titolare e il responsabile del trattamento*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

G. Fares (2021), *The processing of personal data concerning health according to the EU Regulation*, in G. Fares (ed.), "The Protection of Personal Data Concerning Health at the European Level. A Comparative Analysis", Giappichelli, 2021

G. Finocchiaro (2019), *Il principio di* accountability, in R. Caterina (a cura di), "GDPR tra novità e discontinuità", in "Giurisprudenza italiana", 2019

G. Finocchiaro (2012), *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli, 2012

G. Finocchiaro (2008), *Il trattamento dei dati sanitari: alcune riflessioni critiche a dieci anni dall'entrata in vigore del Codice in materia di protezione dei dati personali*, in G.F. Ferrari (a cura di), "La legge sulla privacy dieci anni dopo", Egea, 2008

M. Foglia (2020), *Patients and privacy: GDPR compliance for healthcare organizations*, in "European Journal of Privacy Law & Technologies", 2020, Special Issue

M. Foglia (2018), *Consenso e cura. La solidarietà nel rapporto terapeutico*, Giappichelli, 2018

S. Franca (2023), *I dati personali nell'amministrazione pubblica: attività di trattamento e tutela del privato*, Università degli studi di Trento, 2023

F. Francario (2022), *Protezione dei dati personali e pubblica amministrazione*, in C. Pisani, G. Proia, A. Topo (a cura di), "Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro", Giuffrè, 2022

F. Francario (2021), *Disposizioni "urgenti" in materia di protezione dei dati personali. Brevi note sul trattamento dati per finalità di pubblico interesse*, in "www.giustiziainsieme.it", 26 ottobre 2021

A.M. Gambino, E. Maggio,V. Occorsio (2020), *La riforma del fascicolo sanitario elettronico*, in "www.dimt.it", 22 luglio 2020

L. Gatt, I.A. Caggiano, R. Montanari (ed.) (2021), *Privacy and consent. A legal and UX&HMI approach for data protection*, Università degli Studi Suor Orsola Benincasa, 2021

L. Georgieva, C. Kuner (2020), *sub art. 9*, in C. Kuner, L.A. Bygrave, C. Docksey (eds.), "The EU General Data Protection Regulation (GDPR). A Commentary", Oxford University Press, 2020

M. Granieri (2017), *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, in "Nuove leggi civili commentate", 2017

L. Greco (2019), *Sanità e protezione dei dati personali*, in G. Finocchiaro (a cura di), "La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101", Zanichelli, 2019

P. Guarda (2019), *I dati sanitari*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

P. Guarda (2011), *Fascicolo Sanitario Elettronico e protezione dei dati personali,* Università degli Studi di Trento, 2011

P. Iamiceli (2024), *Consenso al trattamento e giurisprudenza europea: tra tutela dei diritti fondamentali e giustizia contrattuale*, in S. Orlando (a cura di), "Libertà e liceità del consenso nel trattamento dei dati personali", Persona e Mercato, 2024

C. Irti (2022), *Personal Data, Non-personal Data, Anonymised Data, Pseudonymised Data, De-identified Data*, in R. Senigaglia, C. Irti, A. Bernes (eds.), "Privacy and Data Protection in Software Services", Springer, 2022

L. Lessig (1999), *Code and Other Laws of Cyberspace*, Basic Books, 1999

E. Maestri (2015), *Lex informatica. Diritto, persona e potere nell'età del cyberspazio*, Edizioni Scientifiche Italiane, 2015

A. Mantelero (2019), *La gestione del rischio*, in G. Finocchiaro (a cura di), "La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101", Zanichelli, 2019

A. Mantelero (2017), *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (artt. 32-39)*, in G. Finocchiaro (a cura di), "Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali", Zanichelli, 2017

M. Mantovani (2019), *Introduzione l. n. 219/2017*, in A. Barba, S. Pagliantini (a cura di), "Delle persone. Leggi collegate", II, nel "Commentario del Codice civile", diretto da E. Gabrielli, Utet, 2019

R. Messinetti (2019), *Circolazione dei dati personali e autonomia privata*, in N. Zorzi Galgano (a cura di), "Persona e mercato dei dati. Riflessioni sul GDPR", Cedam, 2019

R. Miccú (2021), *Questioni attuali intorno alla digitalizzazione dei servizi sanitari nella prospettiva multilivello*, in "federalismi.it", 2021, n. 5

G. Mirabelli (1993), *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in "Diritto dell'informazione e dell'informatica", 1993

A. Morace Pinelli (2025-a), *Lo spazio europeo dei dati sanitari (reg. UE n. 327/2025)*, in "Nuova giurisprudenza civile commentata", 2025, n. 2

A. Morace Pinelli (a cura di) (2025-b), *Sanità digitale – Regolamento "EHDS" (UE 2025/327) sullo spazio europeo dei dati sanitari. I. Uso dei dati e assetti organizzativi*, Pacini, 2025

S. Patti (1999), *Il consenso dell'interessato al trattamento dei dati personali*, in "Rivista di diritto civile", 1999, n. 2

V. Peigné (2011), *Il fascicolo sanitario elettronico, verso una «trasparenza sanitaria» della persona*, in "Rivista italiana di medicina legale", 2011, n. 6

E. Pellecchia (2020), *Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR*, in "Nuove leggi civili commentate", 2020, n. 2

C. Perlingieri (2024), *Transizione digitale nella sanità ed ecosistema dei dati sanitari: profili ricostruttivi del fenomeno circolatorio e implicazioni sui dati genetici,* in "Tecnologie e diritto", 2024

C. Perlingieri (2022), *eHealth and Data*, in R. Senigaglia, C. Irti, A. Bernes (eds.), "Privacy and Data Protection in Software Services", Springer, 2022

P. Perlingieri (2020), *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, 4ª ed., Edizioni Scientifiche Italiane, 2020

P. Perlingieri (2018), Privacy *digitale e protezione dei dati personali tra persona e mercato*, in "Foro napoletano", 2018, n. 2

P. Perlingieri (2003), *La pubblica amministrazione e la tutela della* privacy. *Gestione e riservatezza dell'informazione nell'attività amministrativa*, in "Annali della Facoltà di Economia dell'Università degli Studi del Sannio", 2003, n. 8

P. Perlingieri (1972), *La personalità umana nell'ordinamento giuridico*, Edizioni Scientifiche Italiane, 1972

A. Pioggia (2021), *Il Fascicolo sanitario elettronico: opportunità e rischi dell'interoperabilità dei dati sanitari*, in R. Cavallo Perin (a cura di), "L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale", Università degli studi di Torino, 2021

A. Pioggia (2011), *Consenso informato ai trattamenti sanitari e amministrazione della salute*, in "Rivista trimestrale di diritto pubblico", 2011, n. 1

F. Piraino (2017), *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in "Nuove leggi civili commentate", 2017, n. 2

F. Pizzetti (2021), *Il procedimento italiano di adeguamento al GDPR e la struttura del Codice novellato*, in F. Pizzetti (a cura di), "Protezione dei dati personali in Italia tra GDPR e codice novellato", Giappichelli, 2021

D. Poletti (2007), *sub art. 75*, in C.M. Bianca, F.D. Busnelli (a cura di), "La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003, n. 196, Codice della privacy", Cedam, 2007

N. Posteraro (2022), *Il fascicolo sanitario elettronico,* in V. Bontempi (a cura di), "Lo Stato digitale nel Piano nazionale di ripresa e resilienza", Università degli Studi Roma Tre, 2022

N. Posteraro (2021), *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in "federalismi.it", 2021, n. 26

N. Posteraro, S. Corso (2023), *The Italian Electronic Health Record (EHR)*, in "European Review of Digital Administration & Law", vol. 4, 2023, n. 1

R. Pucella (2010), *Autodeterminazione e responsabilità nella relazione di cura,* Giuffrè, 2010

G. Resta (2006), *Le nuove dimensioni dei diritti della personalità,* in G. Alpa, G. Resta, "Le persone e la famiglia", I, "Le persone fisiche e i diritti della personalità", nel *Trattato di diritto civile*, diretto da F. Sacco, Utet, 2006

G.M. Riccio (2004), Privacy *e dati sanitari*, in F. Cardarelli, S. Sica, V. Zeno-Zencovich (a cura di), "Il codice dei dati personali. Temi e problemi", Giuffrè, 2004

S. Rodotà (2010), *Il nuovo* habeas corpus*: la persona costituzionalizzata e la sua autodeterminazione*, in S. Rodotà, M. Tallacchini (a cura di), "Ambito e fonti del biodiritto", nel "Trattato di biodiritto" diretto da S. Rodotà e P. Zatti, Giuffrè, 2010

M.A. Sandulli (2023), *Introduzione*, in A. Thiene e S. Corso (a cura di), "La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza", Jovene, 2023

M.A. Sandulli, F. Aperio Bella (a cura di) (2021), *Shaping the Future of Health Law: Challenges for Public Law*, in "federalismi.it", 17 novembre 2021

R. Senigaglia (2023), *Telemedicina ed essenza fiduciaria del rapporto di cura*, in "Persona e mercato", 2023, n. 3

S. Sica (2001), *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in "Rivista di diritto civile", 2001, n. 2

C. Silvano (2023), *La digitalizzazione dei servizi sanitari alla luce del riparto di competenze tra Stato e Regioni. Il caso del Fascicolo Sanitario Elettronico*, in "federalismi.it", 2023, n. 26

B. Sirgiovanni (2020), *Dal consenso dell'interessato alla "responsabilizzazione" del titolare del trattamento dei dati genetici*, in "Nuove leggi civili commentate", 2020, n. 4

S. Slokenberga, K. Ó Cathaoir, M. Shabani (eds.) (2025), *The European Health Data Space. Examining A New Era in Data Protection*, Routledge, 2025

E. Sorrentino, A.F. Spagnuolo (2020), *La sanità digitale in emergenza Covid-19. Uno sguardo al fascicolo sanitario elettronico*, in "federalismi.it", 2020, n. 30

M.G. Stanzione (2022), *La protezione dei dati personali tra «consumerizzazione» della* privacy *e principio di* accountability, in "Comparazione e diritto civile", 2022

A. Thiene (2023), *La regola e l'eccezione. Il ruolo del consenso in relazione al trattamento dei dati sanitari alla luce dell'art. 9 GDPR*, in A. Thiene, S. Corso (a cura di), "La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza", Jovene, 2023

A. Thiene (2021), *sub art. 9, reg. Ue n. 679/2016, I. Profili generali*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), "Codice della privacy e data protection", Giuffrè, 2021

A. Thiene, S. Corso (a cura di) (2023), *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza*, Jovene, 2023

E. Tosi (2019), *Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del* nuovo *Codice Privacy*, in E. Tosi (a cura di), "Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy", Giuffrè, 2019

A.F. Westin (1976), *Computers, Health Records and Citizen Rights*, U.S. Government Printing Office, 1976

V. Zambrano (1999), *Dati sanitari e tutela della sfera privata*, in "Diritto dell'informazione e dell'informatica", 1999, n. 1

F. Zanovello (2023), *Misure di garanzia e rischio di* data breach *in ambito sanitario*, in A. Thiene, S. Corso, (a cura di), "La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza", Jovene, 2023

F. Zanovello (2021), *sub art. 2- septies, d.lgs. n. 196 del 2003*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), "Codice della privacy e *data protection*", Giuffrè, 2021

P. Zatti (2019), *Brevi note sull'interpretazione della legge n. 219 del 2017*, in "Nuove leggi civili commentate", 2019, n. 1

P. Zatti (2018), *Spunti per una lettura della legge sul consenso informato e DAT*, in "Nuova giurisprudenza civile commentata", 2018, n. 1

P. Zatti (2009), *Maschere del diritto volti della vita*, Giuffrè, 2009

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0250 • articolo sottoposto a peer review • pubblicato in anteprima il 3 dic. 2025

Simone Franca

La tutela del privato di fronte al trattamento dei dati da parte della pubblica amministrazione

L'articolo esamina la tutela del cittadino quando il trattamento dei dati è svolto da amministrazioni pubbliche. Viene analizzata la tutela amministrativa del Garante, ponendo in luce le criticità nell'esercizio di questa funzione nei trattamenti di interesse pubblico. Si esamina poi la tutela giurisdizionale concentrandosi su alcuni nodi, ossia giurisdizione esclusiva del giudice ordinario, non appellabilità delle sentenze del giudice, poteri del giudice ordinario. Si considera, infine, il piano della responsabilità tanto nella dimensione civilistica che erariale.

Protezione dei dati personali – Tutela amministrativa – Garante – Tutela giurisdizionale – Responsabilità

Protection of private parties vis-à-vis data processing by public authorities

The article examines the protection available to individuals when personal data are processed by public authorities. It analyzes administrative redress before the Italian Data Protection Authority (Garante), highlighting critical issues that arise when this oversight concerns processing carried out in the public interest. It then turns to judicial remedies, focusing on several key points: the exclusive jurisdiction of the ordinary courts, the non-appealability of first-instance judgments, and the scope of those courts' powers. Finally, it addresses liability, both in its civil-law dimension and in terms of public-accounting liability.

Personal data protection – Administrative remedies – Data Protection Authority – Judicial protection – Liability

L'Autore è ricercatore TD-A in Diritto amministrativo presso la Facoltà di Giurisprudenza dell'Università di Trento

Questo contributo fa parte della sezione monografica *I dati in ambito pubblico tra esercizio della funzione amministrativa e regolazione del mercato*, a cura di Marco Bombardelli, Simone Franca, Anna Simonati

1. Premessa

Il presente contributo[1] ha ad oggetto il tema della tutela di fronte al trattamento dei dati personali. La prospettiva che è assunta non abbraccia tale tema in una prospettiva generale, ma si concentra sullo specifico ambito relativo ai trattamenti operati dalla pubblica amministrazione. A fronte di questi trattamenti – *rectius*, a fronte di trattamenti che sono svolti nell'interesse pubblico –, infatti, anche la tutela si pone in modo differente.

Al fine di delimitare i confini di questa prospettiva occorre svolgere due considerazioni preliminari: la prima sulla natura del diritto alla protezione dei dati personali come situazione giuridica soggettiva; la seconda sulla nozione di tutela.

Per quanto riguarda la prima, assume rilievo la dialettica tra protezione e circolazione dei dati. Il diritto alla protezione dei dati personali, in effetti, non è riassumibile in un *right to be let alone*, secondo, storicamente, la prima accezione del termine *privacy*. Così come chiarito dall'art. 1 GDPR, infatti, il regolamento europeo tutela tanto la protezione delle persone fisiche quanto la circolazione dei dati[2]. Tale circostanza induce a ritenere che di diritto alla protezione dei dati personali si possa discutere solo laddove si dia conto di questa duplice dimensione schiettamente protettiva, ma anche apertamente pro-circolatoria[3]. Calando questa

1. Questo contributo è stato realizzato nell'ambito di una ricerca cofinanziata dall'Unione europea - NextGenerationEU (D.M. n. 737/2021).
2. Si tratta di un approccio già evincibile dalla direttiva 95/46/CE. Sul rilievo della libera circolazione dei dati nella direttiva cfr. Faro 2000, p. 551-552. Si tenga conto che questa prospettiva diventa particolarmente rilevante nell'ambito della società dell'informazione e della legislazione che la riguarda. In tema resta fondamentale Pietrangelo 2007.
3. La natura fondamentale del diritto alla protezione dei dati personali non sposta i termini della questione, essendo ineliminabile e intrinseco a tale diritto il bilanciamento tra esigenze protettive e circolatorie, non potendo essere attribuita a esso una coloritura assoluta. Cfr. in tema Gardini 2024, p. 349 ss.; Tigano 2022, p. 422; Zorzi Galano 2019, p. 35-37; Mulazzani 2019, p. 198. Occorre poi considerare la dimensione del diritto a trattare

lettura nell'ambito dei trattamenti svolti nell'interesse pubblico è facile desumere che la dialettica assume come poli di riferimento esigenze di protezione della persona e di circolazione nell'interesse pubblico.

Giova precisare che la peculiarità di questa dialettica e, conseguentemente, del regime dei trattamenti in ambito pubblico si desume da altri indici positivi contenuti nel GDPR[4].

Passando ora al significato del termine "tutela" è bene rilevare che nelle analisi più risalenti[5], così come in ricostruzioni più recenti[6], rispetto al trattamento dei dati si impiega la locuzione *tutela* dei dati personali. Vi sono ragioni per valorizzare l'uso del termine *tutela* rispetto al trattamento dei dati *tout court*. In effetti, il termine allude alla protezione di un determinato interesse, qualora esso risulti leso o insoddisfatto[7]. Più in generale, e ciò è chiaro dalla lettura dell'art. 1 GDPR, la componente di "protezione delle persone fisiche" è un profilo cruciale (benché non l'unico, come si è detto) che informa la disciplina eurounitaria in materia di protezione dei dati personali. Così, la tutela *nel* trattamento dei dati personali assume un valore euristico che non pare trascurabile, specie perché enfatizza il legame con un interesse.

Il riferimento alla tutela ai fini del presente scritto, tuttavia, va riguardato *rispetto al* trattamento, sotto due profili che conviene tenere a mente. In primo luogo, rileva l'attività del Garante con cui questi è chiamato controllare la conformità dei trattamenti di dati personali già in essere[8] rispetto alla disciplina

dati altrui su cui il rinvio è doveroso a Bravo 2018. Sulla sottovalutazione della dimensione circolatoria come all'origine di un equivoco relativo all'uso del termine *privacy* si v. Ricciuto 2022, spec. p. 24 ss.

4. Nel settore pubblico, il trattamento dei dati personali si fonda normalmente su una norma che attribuisce un compito di interesse pubblico o che fonda un obbligo legale. Inoltre alcune basi giuridiche comuni non trovano applicazione per trattamenti in ambito pubblico: il consenso non è utilizzabile quando esiste uno squilibrio tra titolare e interessato come nel caso in cui titolare sia una autorità pubblica (Cons. 45 GDPR); il legittimo interesse non può fondare trattamenti di autorità pubbliche per l'esercizio dei propri compiti (art. 6, par. 1 GDPR). In aggiunta, i diritti degli interessati non conservano la loro piena esigibilità: ad esempio, la cancellazione dei dati non è ammessa quando il trattamento è necessario per l'interesse pubblico, salvo eccezioni molto limitate (art. 17, par. 3 GDPR). Un'ulteriore peculiarità riguarda la vigilanza: quando il trattamento è svolto da un'autorità pubblica, non si applica il meccanismo europeo dello sportello unico e la competenza resta sempre all'autorità garante dello Stato in cui ha sede l'ente pubblico (Cons. 128 GDPR). Infine, va ricordato che il GDPR lascia agli Stati membri la scelta se assoggettare o meno le amministrazioni pubbliche al sistema sanzionatorio (art. 83, par. 7 GDPR). In tema sia consentito il rinvio a Franca 2023, spec. p. 306 ss.
5. Riferimenti ai problemi di trattamento dei dati personali attraverso le formulazioni *tutela della privacy* o *tutela dei dati personali* si rinvengono, ad esempio, in Arena 1997, p. 505 ss., Clarich 1997, p. 137 ss.; Giannantonio 1999, p. 483 ss.; Giannantonio–Losano–Zeno-Zencovich 1997, *passim*. D'altronde anche la direttiva 95/46/CE era "relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati".
6. L'impiego della formula "tutela dei dati personali" nella letteratura recente si riscontra in Bombardelli 2022, p. 351 ss.; Mantelero 2015, p. 137 ss.; Sica 2016, p. 4; parla di tutela della privacy; Principato 2015, p. 199 ss.
7. In questa prospettiva cfr. Di Majo 1992, p. 360, rispetto al significato generale di tutela. È chiaro che nel diritto romano, tale lemma si sviluppa in un senso più specifico, come tutela dei soggetti inidonei da soli a provvedere ai propri interessi (cfr. Zannini 1992, p. 305 ss.) secondo un'impostazione che è penetrata poi nel diritto privato e che rimane comunque distinta dalla tutela giurisdizionale come intesa ai sensi dell'art. 2907 c.c. su cui si v. ancora Di Majo 1992, p. 361 ss., nonché per un approccio di teoria generale Chizzini 2018.
8. Questa funzione è attribuita dal combinato disposto degli artt. 57, par. 1, lett. a) del GDPR e dall'art. 154, co. 1, lett. a) del Codice privacy. La prima disposizione declina la funzione essenzialmente come attività consistente nel sorvegliare e nell'assicurare l'applicazione del Regolamento. La seconda disposizione parla invece di "controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile". La latitudine particolarmente ampia, in particolare della prima formulazione, ha portato a rilevare una significativa compressione del principio di tipicità dell'azione amministrativa (Midiri 2019, p. 989).

eurounitaria e nazionale[9]. Si tratta in questo caso di una tutela amministrativa, nella specie riconducibile all'esercizio di poteri di tipo non giurisdizionale e qualificabili come poteri di vigilanza. In secondo luogo, assume rilievo la tutela propriamente giurisdizionale, esercitata dal giudice ordinario, il quale è competente per lo svolgimento del sindacato sul trattamento dei dati personali, anche qualora svolto da pubbliche amministrazioni o, più in generale, nell'interesse pubblico. Saranno queste due dimensioni a fungere da guida nel presente scritto.

2. La tutela amministrativa del Garante. L'approccio formalista e la svalutazione dell'interesse pubblico

Nell'ambito dell'attività di tutela amministrativa il Garante, tramite poteri ispettivi, correttivi e sanzionatori, esercita una funzione di vigilanza[10].

Si tratta di una funzione che non può essere qualificabile come connotata da neutralità. In effetti, il Garante nell'esercizio di tale funzione non si limita a fungere da arbitro neutrale[11] con riguardo a una specifica controversia – anche in sede di reclamo – dato che interviene nel perseguimento dello specifico interesse teso ad assicurare la tutela del diritto alla tutela dei dati personali di cui è investito[12]. Ad ogni buon conto, il fatto che il Garante persegua lo specifico interesse alla protezione dei dati personali fa sì che, per verificare la sussistenza di una lesione, debba valutare come è stato svolto il bilanciamento tra la protezione delle persone fisiche e le esigenze legate alla libera circolazione dei dati[13].

Va, inoltre, precisato che, qualora il trattamento sia operato sulla base di un obbligo di legge o

9. Tale formulazione è quella che si evinceva e si evince tutt'ora dalla Parte terza del Codice privacy: qui, infatti, il Titolo I è dedicato alla tutela amministrativa e giurisdizionale dell'interessato. La formulazione anodina della funzione esercitata dal Garante si deve, come si vedrà *infra*, alla commistione tra profili tipici di funzioni diverse.
10. Si consideri che sussistono diversi elementi per ritenere che l'attività di tutela amministrativa del Garante sia qualificabile come attività di vigilanza sulla base di una valutazione di ordine soggettivo, basata sull'indipendenza dell'ente vigilante, e di tipo oggettivo, fondata sul fatto che oggetto della vigilanza sia un'attività e non uno o più atti. In primo luogo, il Garante è autorità dotata di indipendenza, qualifica solitamente attribuita agli enti vigilanti. In secondo luogo, il Garante non sindaca specifici atti (come avviene nel caso del controllo), ma, piuttosto, interviene con riferimento ad attività. Sul rilievo dell'indipendenza e del tipo di attività svolta per qualificare la funzione di vigilanza cfr., da ultimo, De Bellis 2021, p. 343. Più in generale, sulla qualificazione di tale attività si v. Amorosino 2004, p. 25 ss.; Antonioli 2013, p. 673 ss.; Stipo 1994; Valentini 1993, p. 702 ss.
11. Su tale concetto è imprescindibile Sandulli 1964/1990, p. 259 ss. Più in generale, sulla configurabilità delle funzioni delle autorità indipendenti come funzioni neutrali cfr., in part., Caianiello 1988, p. 554; Torchia 1996, p. 65; Perez 1996, p. 115 ss.; Vesperini 1990, p. 415 ss. Recentemente, per un'analisi esaustiva della tesi della neutralità cfr. Bruti Liberati 2019, p. 31 ss. Sul fatto che nell'ipotesi di amministrazione contenziosa le autorità indipendenti esercitino una funzione neutrale, ponendosi al di fuori dell'assetto di interessi propri dei soggetti in lite, si v. Caputi Jambrenghi 2017, p. 273.
12. Rispetto alla circostanza secondo cui il Garante non agisce neutralmente, ma nel perseguimento dell'interesse alla tutela dei dati personali cfr. Gola 2011, p. 241, che si riferisce alle ipotesi in cui il Garante interveniva su ricorso. Sul particolare ruolo del Garante rispetto alla tutela della privacy cfr. Merusi 2000, p. 54. Nel caso del Garante, dunque, sembra concretizzarsi l'esercizio di una funzione vigilanza in cui, come ben dimostrato da Caputi Jambrenghi 2017, p. 272-273, rispetto ad ipotesi non relative all'esercizio di funzioni giustiziali, le autorità indipendenti non agiscono in modo indifferente rispetto agli interessi in gioco. Si consideri anche l'opinione di Della Cananea 2005, p. 615 secondo cui anche la neutralità non può equivalere all'indifferenza rispetto agli interessi particolari e a come ciascuno di essi condiziona la realizzazione degli obiettivi della regolazione, anche rispetto alla risoluzione di controversie.
13. In effetti, se si immagina il caso dell'amministrazione titolare del trattamento vi saranno senz'altro casi in cui questa è tenuta ad applicare in modo vincolato regole in materia di protezione dei dati (ad esempio, rispetto all'accesso ai propri dati personali che un interessato proponga rispetto ad una procedura ad evidenza pubblica che lo riguarda). In simili casi, l'accertamento di una violazione da parte del Garante non pone problemi,

per l'esercizio di un compito di interesse pubblico – come avviene, di regola[14], nell'ambito dei trattamenti in ambito pubblico –, la competenza esclusiva dell'autorità Garante italiana non è derogabile, non potendo operare il meccanismo dello sportello unico[15].

Ciò posto, concentrandosi su come la funzione di tutela amministrativa è esercitata dal Garante può osservarsi come essa sia orientata a tutelare secondo una prospettiva che dà particolare rilevanza alla sussistenza di violazioni indipendentemente dal grado di lesività delle stesse.

Nella prassi del Garante emerge, infatti, un'attenzione anche molto capillare e minuziosa a certe violazioni – si pensi ai rilievi puntuali che sono svolti sulle informative – in cui passa in secondo piano la salvaguardia della persona fisica, rappresentante, come detto, una delle finalità delle regole di protezione. In un simile contesto, l'utilizzo di poteri sanzionatori si rivela indifferente all'apprensione della lesività delle violazioni compiute. La violazione delle regole in materia di trattamento dei dati personali, in effetti, può avere una natura meramente formale e non arrecare un pregiudizio rilevante alla sfera dell'interessato. Si pensi, a titolo esemplificativo, all'erronea indicazione dei riferimenti relativi ai diritti degli interessati che, pur rappresentando una violazione della disciplina, pare avere un impatto quantomeno dubbio, quanto alla sua incidenza, sulla sfera giuridica del soggetto interessato[16].

È pur vero che il sistema di protezione dei dati personali non prevede che le violazioni possano essere lamentate dagli interessati solo per specifiche finalità o addirittura che il sistema di protezione sia fondato sulla riparazione di un

così come quando un trattamento venga operato da un'amministrazione in contrasto con quanto previsto nell'ambito di un atto amministrativo generale *ex* art. 2-*ter*, co. 1 Codice privacy o con le risultanze di una valutazione di impatto. Tuttavia, vi possono essere casi in cui l'amministrazione è chiamata ad operare un bilanciamento tra la protezione dei dati personali e gli interessi sottoposti alla sua cura. Cfr. Cerbo 2012, p. 754-755, il quale ritiene che non di rado i provvedimenti del Garante siano connotati da discrezionalità; Gola 2011, p. 239, ove afferma che il Garante opera valutazioni relative al bilanciamento fra esigenze di riservatezza ed esigenze di informazione e comunicazione. Sul collegamento tra il perseguimento di un interesse pubblico specifico e la titolarità di poteri discrezionali con riguardo alle autorità indipendenti, intese come non titolari di funzioni neutrali cfr. Caputi Jambrenghi 2017, spec. p. 253 ss. Si tenga presente, comunque, che la scelta relativa alla misura della soddisfazione di più interessi, anche nel perseguimento di un interesse pubblico specifico, non implica l'esercizio di un potere discrezionale, come rilevato, con riguardo alle autorità indipendenti, in Torricelli 2023, p. 1400 ss. Si noti, peraltro, che la sussistenza di poteri di tipo discrezionale determina un'attenuazione dell'indipendenza delle autorità indipendenti, come rilevato in Bruti Liberati 2019, p. 86.

14. Si tratta di ipotesi in cui il trattamento è strumentale ad atti di tipo non autoritativo. Per tali ipotesi sia consentito rinviare a Franca 2023, p. 318.
15. Si tratta del meccanismo che facilita la cooperazione fra autorità nel caso dei c.d. trattamenti transfrontalieri, stabilendo la possibilità di individuare un'autorità di controllo come autorità capofila e come soggetto che funge da punto di riferimento per i soggetti che operano come titolari di trattamenti transfrontalieri. Su tale istituto cfr. Bombardelli 2022, p. 372-373; Cardarelli 2021, p. 757 ss.; Ferola 2019, p. 1033 ss.; Macchia–Figliolia 2018, p. 432 ss.
16. A titolo esemplificativo, si v. il caso della sanzione di 4.000 euro ad un Comune perché aveva una informativa di secondo livello difficilmente reperibile e comunque con riferimenti non aggiornati al GDPR (Garante Privacy, provv. 27 novembre 2024, doc. web n. 10097307). Indubbiamente, il mancato aggiornamento dei riferimenti normativi è una marchiana violazione (che mostra anche incuria nella *compliance*), ma è difficile non ritenere che la violazione abbia carattere formale. Basti a tal riguardo svolgere un paragone con l'approccio della giurisprudenza amministrativa sull'omessa indicazione di tempi e autorità competenti per il ricorso. Tale violazione è valutata come una mera irregolarità valevole semmai ai fini della rimessione in termini (Cons. Stato, sez. V, 15 novembre 2012, n. 5772; Tar Umbria, Sez. I, 29 maggio 2024, n. 397). Anche la giurisprudenza civile ha ritenuto che l'omessa informazione su come ricorrere avverso la cartella esattoriale non incida sulla validità dell'atto, rilevando piuttosto come errore scusabile in caso di ricorso tardivo o presentato al giudice non competente (Cass., sez. trib., 16 settembre 2021, n. 25023).

pregiudizio, essendo questo un profilo che rileva semmai sul piano della tutela risarcitoria, su cui si tornerà *infra*.

Occorre però considerare che l'assunzione di una prospettiva tesa ad accentuare il rilievo di violazioni formali rischia di ripercuotersi sulla cura degli interessi perseguiti tramite il trattamento in particolare, nell'ambito che ci occupa, degli interessi pubblici. Così facendo, il rischio è di concepire il diritto alla protezione dei dati personali come una posizione giuridica di fatto assoluta, che in un bilanciamento con gli interessi pubblici non può che prevalere[17].

Alcuni esempi concreti possono chiarire la problematicità di quanto si va affermando.

Un primo caso da considerare è quello relativo al cd. bonus covid. In questa fattispecie il problema del trattamento riguardava l'uso di codici fiscali ricavati dai dati in rete di parlamentari e titolari di cariche in enti locali per finalità di controllo sull'erogazione dei bonus. L'INPS voleva evitare che le scarse risorse a disposizione fossero sperperate e quindi ha imbastito un'attività di controllo utilizzando dati pubblici per ricavare codici fiscali. Il Garante ha sanzionato pesantemente l'INPS (300.000 euro), paventando anche un rischio elevato al trattamento dei dati degli interessati, censurando il trattamento svolto alla luce di numerosi principi del trattamento (esattezza, responsabilizzazione, minimizzazione, liceità). La decisione del Garante è stata poi annullata dal tribunale di Roma[18], il quale ha ritenuto non condivisibile la posizione del Garante. Ciò che preme in questa sede evidenziare, al di là dei condivisibili rilievi del Tribunale di Roma – che puntualmente valorizza la situazione emergenziale in cui si trovava a decidere l'INPS –, è il fatto che le violazioni individuate dal Garante parevano foriere di conseguenze negative del tutto ipotetiche. Si pensi alla posizione dei soggetti che avevano visto respingere la propria domanda al bonus, i cui codici fiscali sono stati trattati per svolgere i controlli. Non si può pensare che vi sia una reale lesione nei confronti della privacy di questi soggetti, posto che, peraltro, nello svolgimento di un controllo manuale (e non automatico) è facile che accada di scandagliare anche domande non rilevanti.

Ancor più esplicita è la sentenza del tribunale di Udine rispetto al trattamento di profilazione sanitaria svolto da tre aziende sanitarie friulane nell'ambito dell'emergenza pandemica[19].

La fattispecie riguardava la profilazione per identificare individui suscettibili di veder insorgere complicanze. Nella sentenza (sebbene recentemente cassata) il giudice si chiede "quale pregiudizio per i diritti e le libertà dei pazienti possa derivare dalla predisposizione di elenchi di assistiti in condizioni di maggiore vulnerabilità, in base ad informazioni già presenti nei database delle Aziende Sanitarie e già noti ai medici di base, tenuto conto della finalità, già più volte ribadite, di tale trattamento (potenziamento e programmazione degli

17. Peraltro, si pone un ulteriore problema di ordine sistematico dal momento che il Garante finisce, in via surrettizia, per definire una posizione nel merito, cioè rispetto all'assunzione di soluzioni che invadono il merito della decisione delle autorità amministrative titolari del trattamento (cfr. Francario 2023, par. 2.2; Tigano 2022, p. 422; se si vuole, Franca 2023, p. 215 ss.). Resta fondamentale il rilievo dubitativo di Falcon 2015 rispetto ai rimedi giustiziali (p. 260): "se l'amministrazione che decide il ricorso fosse realmente altra cosa rispetto a quella che agisce, allora che cosa la legittimerebbe ad assumere soluzioni di merito? Più diventa 'altra cosa' meno è legittimata a decidere nel merito in luogo di quella cui è attribuito il compito di base".

18. Trib. Roma, sez. XVIII, 24 marzo 2022, n. 4735, su cui si cfr. Francario 2022, par. 2.1. e par. 2.2; Tigano 2022, p. 424 ss.; Lorè 2022.

19. La vicenda riguardava un trattamento operato da tre aziende ospedaliere universitarie. Il Garante ha ritenuto che le tre aziende fossero tre autonomi titolari, pertanto, le ha separatamente sanzionate (con provvedimenti del 15 dicembre 2022, nn. 9844989, 9845312 e 9845156). Ciò ha portato all'impugnazione delle sanzioni davanti ai tribunali competenti, ossia quelli di Udine, Pordenone e Trieste. Allo stato sono state adottate le sentenze del Tribunale di Udine del 20 novembre 2023, r.g. n. 308/2023 e del Tribunale di Pordenone del 10 ottobre 2023, n. 228/2023. La seconda ha annullato la sanzione del Garante ritenendo che il titolare fosse la Regione Friuli-Venezia Giulia. La sentenza del Tribunale di Udine ha anche chiarito come nessuna delle violazioni rilevate dal Garante fosse fondata.

interventi di prevenzione e cura nell'ambito del contesto emergenziale pandemico)"[20].

Qui la fattispecie è complessa e senz'altro vi sono alcune criticità che sono state colte nella sentenza della Corte di Cassazione[21].

Preme però osservare come entrambe le vicende siano sintomatiche di un approccio in cui il rilievo dato al rispetto della conformità ai principi del trattamento (esigenza senz'altro commendevole) tenda a far scendere in secondo piano l'interesse pubblico cui il trattamento è funzionale. Ciò non vuol dire, evidentemente, che la finalità pubblicistica giustifichi una più circoscritta tutela del diritto alla protezione dei dati personali. Piuttosto significa che tale tutela va necessariamente ambientata in un contesto pubblicistico dove anche principi fondamentali del trattamento, come quello di minimizzazione, necessitano di un almeno tendenziale temperamento – quando non di una rilettura – nel senso di valorizzare l'efficacia dell'azione amministrativa e, più in generale, il rilievo di principi altrettanto cogenti che governano l'azione amministrativa[22].

Una simile esigenza è peraltro chiara anche a fronte di altri trattamenti come quelli legati alla trasparenza amministrativa. Anche in questo frangente, infatti, l'impostazione del Garante tesa a dare preminenza alle esigenze legate alla privacy rischia di limitare fortemente il ruolo della conoscibilità delle informazioni, altrettanto rilevante per lo sviluppo della persona umana[23].

3. I caratteri della tutela giurisdizionale e le sue criticità

Nell'approcciare il tema della tutela giurisdizionale occorre prendere atto del tenore affatto particolare con cui questa è stata strutturata dal legislatore.

In primo luogo, occorre rilevare che il giudice ordinario è competente per tutte le controversie "comunque riguardanti l'applicazione della normativa in materia di protezione dei dati personali, nonché il diritto al risarcimento del danno ai sensi dell'articolo 82 del medesimo Regolamento", ai sensi dell'art. 152 Codice Privacy[24]. Accantonando per ora le questioni relative al risarcimento del danno da illecito trattamento, occorre soffermarsi sulla portata del riferimento operato a tutte le controversie riguardanti l'applicazione della normativa in materia di protezione dei dati personali. Fra gli interpreti[25] si è evidenziato che il legislatore avrebbe inteso prevedere un'ipotesi di giurisdizione esclusiva dinanzi al giudice ordinario, per cui la materia apparterrebbe *in toto* a siffatto giudice, indipendentemente dalle posizioni giuridiche soggettive che possono venire in rilievo.

In secondo luogo, occorre rilevare che il rito del giudizio in materia di protezione dei dati personali appartiene ai riti semplificati e trova la propria disciplina, principalmente, nell'art. 10, del d.lgs. 1°

20. Cfr. Trib. Udine, 20 novembre 2023, r.g. n. 308/2023, p.to III-d). Non si condivide, tuttavia, l'uso del termine pregiudizio che pare evocativo di un giudizio di responsabilità.
21. Si allude alla sentenza Cass. civ., sez. I, 6 marzo 2025, n. 6067, che ha cassato con rinvio la sentenza del Tribunale di Udine, riconoscendo l'ASUFC quale titolare del trattamento, escludendo la qualificazione della profilazione sanitaria come trattamento secondario, negando la necessarietà delle operazioni svolte e rilevando, inoltre, la violazione dell'art. 35 GDPR in materia di valutazione di impatto.
22. Per tale impostazione, se si vuole, si v. Franca 2023, p. 327 ss.
23. Sul punto si v. Carloni 2022, p. 262-263. Come rileva Simonati 2023, p. 9 non è censurabile solo la pubblicazione di informazioni riservate, ma anche "l'occultamento indiscriminato di dati personali non riservati".
24. Il testo integrale del menzionato articolo dispone che "Tutte le controversie che riguardano le materie oggetto dei ricorsi giurisdizionali di cui agli articoli 78 e 79 del Regolamento e quelli comunque riguardanti l'applicazione della normativa in materia di protezione dei dati personali, nonché il diritto al risarcimento del danno ai sensi dell'articolo 82 del medesimo Regolamento, sono attribuite all'autorità giudiziaria ordinaria". È stato rilevato che l'uso del "comunque" pare alludere al fatto che siano attratte nella giurisdizione esclusiva del giudice ordinario anche controversie riguardanti normativa diversa pur sempre connessa a quella della protezione dei dati: sul punto, si v. Pelino 2019, p. 434.
25. Enfatizza la necessità di leggere la regola di giurisdizione come attributiva di una giurisdizione esclusiva Midiri 2017, p. 298 ss.

settembre 2011, n. 150. Questo rito ha diverse peculiarità: il fatto di essere ispirato al rito del lavoro, la previsione di un termine di decadenza (in caso di impugnazione di un provvedimento del Garante), l'obbligo di notifica al Garante, ma anche un elemento molto peculiare, ossia la non appellabilità della sentenza che definisce la controversia[26]. In base alla legge, è esclusa l'appellabilità delle pronunce dei giudici di merito di primo grado che intervengano sul trattamento dei dati. Di conseguenza, le sentenze del tribunale in materia di protezione dei dati possono essere oggetto di gravame solo con impugnazione in Cassazione.

Da ultimo, il giudice ordinario in questi casi non è avvinto dai limiti usuali rispetto alla cognizione dei provvedimenti della pubblica amministrazione. In queste controversie, il giudice ordinario non si trova nella consueta situazione di poter unicamente conoscere dei provvedimenti amministrativi ai fini dell'esercizio dei poteri di disapplicazione (in base all'art. 4 dell'all. e) alla l. 2248/65), ma può disporre, per usare lo stesso linguaggio dell'all. e), la "modifica" e la "revoca" del provvedimento stesso, nella prospettiva dell'esercizio di una giurisdizione piena[27]. Oltre a ciò, il giudice può disporre la condanna al risarcimento del danno, azione che, con l'entrata in vigore del GDPR, risulta essere in tutto disciplinata da quest'ultimo, segnatamente all'art. 82.

Alla luce di questi aspetti, preme soffermarsi su alcune criticità, particolarmente evidenti.

Ciò detto passo ora all'esame delle criticità di questi diversi aspetti: giurisdizione esclusiva, non appellabilità della sentenza e dimensione dei poteri del giudice ordinario.

3.1. La temperata esclusività della giurisdizione del giudice ordinario nelle controversie pubblicistiche

Sul piano della giurisdizione occorre rilevare, anzitutto, che la scelta per la giurisdizione esclusiva non è così comune, sul piano comparato, almeno con riguardo a sistemi in cui è riconosciuta una giurisdizione speciale. Se si considera, ad esempio, il sistema tedesco si evincerà che si è riconosciuta la giurisdizione del giudice amministrativo per la lesione di diritti sul trattamento, come il diritto di accesso ai dati personali nei confronti di amministrazioni titolari del trattamento[28]. Il legislatore tedesco ha peraltro attribuito la giurisdizione in controversie riguardanti i dati personali ad altri giudici speciali come il *Sozialgericht*, rispetto ai trattamenti di "dati sociali" (*Sozialdaten*)[29] e al *Finanzgericht* rispetto ai trattamenti operati dall'amministrazione finanziaria (*Finanzbehörden*)[30].

A prescindere da ciò, occorre rilevare che l'esclusività della giurisdizione è meno rigida di quanto possa apparire.

Sul punto occorre considerare il problema rappresentato dall'adozione di un provvedimento amministrativo in violazione degli atti normativi che disciplinano la materia della protezione dei dati, ossia il GDPR e il codice privacy.

Al di fuori delle controversie in materia di accesso – dove sussiste un'altra giurisdizione esclusiva, del giudice amministrativo[31] – la situazione è piuttosto complessa, perché la violazione delle regole in materia di protezione dei dati potrebbe essere rilevante, in via strumentale, per lamentare

26. Per un inquadramento generale di questi profili cfr. Pagni 2012; Licci 2011, p. 105 ss. Con particolare riferimento al rito, in seguito all'adeguamento al GDPR, cfr. Lubello 2021, p. 1706 ss. e Mazza 2021, p. 966 ss. con particolare riferimento alle modifiche operate con d.lgs. 101/2018.

27. Sulla natura piena della giurisdizione esercitata dal giudice in siffatte controversie si v. in part. Midiri 2017, p. 302-303; Figorilli 2002, p. 281 ss. Si tratta di una terminologia presente già in Sandulli 1989, p. 1283, 1326, 1301, 1337.

28. Per alcuni esempi in questo senso cfr. *Verwaltunsgericht* Bayreuth, 28 febbraio 2019 - B 9 K 18.1014; *Bundesverwaltungsgericht*, 9 dicembre 2022 - 10 B 2.22.

29. Cfr. il § 81b del *Sozialgesetzbuch. Zehntes Buch Sozialverwaltungsverfahren und Sozialdatenschutz* (SGB X).

30. Cfr. il § 32i dell'*Abgabenordnung* (AO).

31. Non avrebbe senso, in questa prospettiva, creare una differenziazione nel caso del controinteressato all'accesso che fa valere la lesione del proprio diritto alla riservatezza, posto che, diversamente opinando, potrebbero radicarsi due giurisdizioni parallele suscettibili di condurre a due giudicati fra loro confliggenti. In questa prospettiva, si v. De Donno 2019, p. 369. Il tema diventa più critico rispetto all'accesso civico. Sia consentito rispetto a tale problema rinviare a Franca 2023, p. 293 ss. e alle fonti ivi menzionate.

la lesione di una posizione di interesse legittimo. Si pensi al caso relativo a dati personali raccolti in assenza di una base giuridica e utilizzati nell'ambito di un'istruttoria procedimentale. La violazione della liceità del trattamento (ad esempio, per mancanza di base giuridica o errata individuazione della base giuridica) potrebbe essere sollevata per far valere l'illecita acquisizione di informazioni e documenti nell'ambito di un procedimento disciplinare o di un procedimento sanzionatorio.

Ricadere nell'una o nell'altra giurisdizione non è indifferente specie perché sembrerebbe che il giudice amministrativo possa contare su una più consolidata esperienza nel bilanciamento tra i diversi interessi in gioco.

A tale riguardo è sufficiente considerare la giurisprudenza consolidatasi nel tempo rispetto al bilanciamento tra trasparenza e riservatezza. Certo non mancano orientamenti criticabili, ma generalmente il giudice amministrativo, per quanto riguarda l'accesso documentale, si limita a rilevare le lacune sul piano motivazionale dell'istanza di accesso[32] o del diniego[33], accertando in astratto il nesso di strumentalità tra l'interesse giuridicamente rilevante del richiedente l'accesso e il documento oggetto della pretesa ostensiva[34], suggerendo altresì soluzioni "informali" al contrasto tra accesso e privacy, tramite interlocuzioni tra accedente e amministrazione[35].

Nella giurisprudenza sull'accesso civico, invece, l'orientamento dominante appare poco aperto alla considerazione dell'interesse pubblico benché vi sia anche parte della giurisprudenza che impiega il cd. *public interest test* per svolgere un bilanciamento più accurato[36].

Un esempio significativo si ha poi nel caso del TAR Lazio, sez. I, 17 aprile 2025, n. 7625, in cui il giudice amministrativo ha reso una pronuncia di grande rilievo sul fronte del trattamento di dati personali in ambito pubblico. Con la sentenza si è posto condivisibilmente un argine alla prassi dell'oscuramento indiscriminato delle pronunce contenute nella banca dati nazionale del merito. In questa sede il TAR ha chiarito il rilievo della comprensibilità delle pronunce. In difetto della comprensibilità, non è possibile, secondo il giudice, operare correttamente, ad esempio, la tecnica del *distinguishing*. Nella lettura operata dal collegio giudicante, l'oscuramento indiscriminato incide negativamente sulla difesa del proprio assistito, dal momento che la predisposizione delle difese presuppone di poter comprendere la portata di precedenti arresti della giurisprudenza[37]. Ecco, dunque, che il giudice amministrativo si mostra consapevole del fatto che la logica difensiva della privacy

32. Si considerino, in tal senso, TAR Lazio - Roma, sez. III, 28 settembre 2021, n. 9981; Cons. Stato, sez. V, 9 marzo 2020, n. 1664.
33. Si vedano, ad esempio, TRGA Trentino-Alto Adige - Trento, 13 luglio 2023, n. 125; TAR Lombardia - Milano, sez. II, 30 luglio 2021, n. 1364; TAR Campania - Salerno, sez. I, 22 luglio 2019, n. 1372, le quali non ritengono sufficiente la mera allegazione dell'opposizione del controinteressato per negare l'istanza ostensiva.
34. Per quanto riguarda la sussistenza del nesso di strumentalità tra accesso ai documenti e tutela di un proprio interesse il giudice amministrativo afferma che "non spetta alla Pubblica Amministrazione valutare l'effettiva utilità degli atti richiesti […], bensì solo verificare l'attinenza degli stessi all'interesse che l'istanza intende tutelare" (in tal senso, cfr. TAR Emilia Romagna - Bologna, sez. II, 12 maggio 2023, n. 291; in termini, Cons. Stato, sez. VI, 1° marzo 2023, n. 2193; Cons. Stato, sez. III, 25 febbraio 2022, n. 1342). Non sono invece condivisibili gli orientamenti tesi a valutare nel merito le scelte difensive del richiedente l'accesso, come in Consiglio di Stato, sez. III, 31 dicembre 2020, n. 8543: sulle criticità di quest'ultimo orientamento cfr. Piazza 2021.
35. Cfr. TAR Lazio - Roma, sez. III-*quater*, 4 luglio 2022, n. 9125 dove il collegio, adito in sede di ottemperanza, ritiene che "il richiesto accesso debba essere consentito in forma dialettica con la parte ricorrente proprio al fine di accertare se la documentazione sanitaria contenga gli accertamenti per cui è causa". Il tema si pone anche rispetto all'amministrazione attiva e la tutela della privacy, laddove non adeguatamente dosata, rischia di ostacolare la comprensibilità dell'informazione pubblica e così condurre ai rischi di disinformazione legati all'uso di un linguaggio non chiaro; su questo tema si v. l'interessante lavoro di Pietrangelo 2020, p. 350 ss.
36. Cfr. TAR Lazio - Roma, sez. III-*quater*, 4 luglio 2022, n. 9125.
37. Cfr. TAR Lazio, sez. I, 17 aprile 2025, n. 7625, spec. p.to 30.

rischia di porre in ombra non solo interessi pubblici, ma anche valori connotati da una logica spiccatamente garantisca e, comunque, di rilevanza costituzionale, come il diritto di difesa in giudizio (art. 24 Cost.).

3.2. Il problema della non appellabilità

Come già chiarito, le sentenze dei giudici di merito aditi direttamente o dopo il ricorso al Garante sono ricorribili solo in Cassazione. Come noto, nel sistema costituzionale italiano non è garantito il doppio grado di giurisdizione di merito[38] e ciò ha impedito che recentemente una questione di legittimità costituzionale relativa a tale sistema superasse il vaglio di non manifesta infondatezza[39]. È però da rilevare che questa limitazione dell'appellabilità rappresenta un problema non trascurabile sul piano dell'effettività della tutela. Ciò si rende particolarmente evidente a fronte di fattispecie, quali quelle che coinvolgono amministrazioni pubbliche come titolari del trattamento. In queste ipotesi, infatti, non poche controversie originano da architetture di trattamenti molto articolate, anche tramite l'utilizzo di atti amministrativi generali. Si pensi, in questa prospettiva, al già menzionato caso relativo al trattamento di profilazione sanitaria operato dalle tre aziende ospedaliere friulane: in questo caso il trattamento, assai articolato, è stato disciplinato minuziosamente con apposita delibera della giunta regionale. In questo caso, la corretta ricostruzione del fatto rappresenta un dato necessario e lo si coglie se si confronta l'analisi svolta dal Tribunale di Udine[40] con quella della Cassazione[41] che si è recentemente pronunciata cassando la sentenza del tribunale di Udine.

A parere di chi scrive la motivazione della sentenza della Cassazione, che pure ha il merito di evidenziare alcune criticità della sentenza cassata, non appare sempre fluida e lineare e ciò dipende da una non totale convergenza rispetto alla ricostruzione del fatto operata dal tribunale di Udine. Tuttavia, tale ricostruzione non è messa in discussione da parte della Cassazione, né potrebbe esserlo dal giudice di legittimità.

Non sfugge certo che la Cassazione possa cassare la sentenza di primo grado con rinvio – d'altronde così è stato disposto rispetto alla menzionata sentenza del Tribunale di Udine –, così consentendo una rinnovata analisi del fatto. Tuttavia, occorre anche tenere in considerazione che fatto e diritto non sono elementi di una fattispecie integralmente scorporabili e separabili tra loro. Senza una chiara perimetrazione del fatto[42], infatti, il rischio è che la parte in diritto risulti meramente speculativa e che non si riesca a operare correttamente la qualificazione giuridica. Senza contare che eventuali carenze istruttorie, ad esempio rispetto alla ricostruzione del trattamento, potrebbero incidere sulla reale tutela delle parti, tanto degli interessati, quanto dei soggetti titolari del trattamento.

3.3. I poteri del giudice ordinario: una giurisdizione davvero piena?

L'ampiezza dei poteri di cui dispone il giudice ordinario in questa ipotesi di giurisdizione esclusiva, come già rilevato, sembra testimoniare la pienezza della tutela offerta, impedendo che si possano

38. Su tale circostanza cfr., fra le molte, Corte cost., 29 ottobre 2009, n. 274; 24 luglio 2009, n. 242; 21 febbraio 2001, n. 421; 28 giugno 1995, n. 280; ordinanze n. 316 del 2002 e n. 421 del 2001,; più recentemente, si v. Corte cost., 26 febbraio 2020, n. 34.

39. Si allude a Cass. civ., sez. I, ord.10 giugno 2021, n. 16402.

40. Si fa riferimento alla già menzionata sentenza Trib. Udine, 20 novembre 2023, r.g. n. 308/2023; cfr. pure, sulla medesima vicenda Trib. Pordenone, 13 ottobre 2023, r.g. n. 228/2023, in cui l'ordinanza-ingiunzione del Garante è annullata sul rilievo che il Garante avrebbe erroneamente individuato il titolare nell'azienda sanitaria invece che nella Regione.

41. Cfr. la già richiamata Cass. civ., sez. I, 6 marzo 2025, n. 6067.

42. È doveroso richiamare nuovamente TAR Lazio, sez. I, 17 aprile 2025, n. 7625, dove si afferma "va rilevato – richiamando l'antico brocardo *da mihi factum, dabo tibi ius* – che per intendere la portata di una pronuncia giurisdizionale è doverosa l'esatta definizione della vicenda fattuale: in assenza dalla comprensione di quest'ultima, infatti, il ragionamento giuridico si presenterebbe totalmente speculativo, divenendo oggetto d'interesse puramente teoretico".

opporre alla decisione di tale giudice limiti rispetto alla sindacabilità del merito sia dinanzi ai provvedimenti del Garante che a quelli dell'amministrazione titolare[43]. Si potrebbe dunque ritenere che il giudice ordinario emerga come dotato di poteri che possono soddisfare il privato anche in modo più "pieno" rispetto a quanto possa fare il giudice amministrativo.

Ciò detto occorre considerare in prima battuta che questi poteri giudiziari non sono necessari in tutta una serie di attività (ad esempio, quelle relative alla trasparenza, tramite la pubblicazione di documenti e informazioni). In caso di illecita diffusione dei dati il giudice – ammesso che l'amministrazione non abbia già proceduto in tal senso prima o durante il giudizio – si limiterà a rimuovere i dati personali illecitamente pubblicati. In concreto, ciò si tradurrà in un'ingerenza del giudice piuttosto limitata nel potere dell'amministrazione, quando la diffusione sia frutto di attività vincolata.

In aggiunta, bisogna tener conto che anche se i poteri del giudice ordinario sono concepiti per intervenire su atti non solo del Garante, ma pure dell'amministrazione titolare, il giudizio avviene di rado in via immediata[44]. Come pronosticato da attenta dottrina[45] e come emerge dalle relazioni del Garante[46], l'opzione del giudizio in via immediata è seguita raramente.

Di conseguenza il giudizio si struttura come giudizio di opposizione all'ordinanza-ingiunzione del Garante[47]. Nel caso in cui il giudice accolga l'opposizione al provvedimento del Garante, allora si limiterà ad annullare quest'ultimo e non anche eventuali atti dell'amministrazione titolare che saranno invece considerati conformi. Nel caso invece in cui il giudice rigetti l'opposizione, si limiterà a confermare il provvedimento reso

43. Preme precisare una circostanza, oggetto di dibattito in passato, relativa alla portata dell'eccezione rispetto ai limiti interni in questo giudizio. Si era infatti posta la questione relativa alla possibilità che i limiti interni fossero ritenuti applicabili unicamente al caso dell'opposizione a provvedimenti del Garante e non anche ai casi in cui venisse in rilievo un provvedimento in ipotesi differenti, quali quelle, ad esempio, di provvedimento emanato dall'amministrazione titolare o responsabile del trattamento, avente un'incidenza sul piano della protezione dei dati. Il dubbio esegetico era prevalentemente dovuto ad un difetto sul piano della confezione della disciplina normativa. Il problema evidenziato era tutt'altro che marginale. Apprezzabilmente, la dottrina più avvertita suggeriva il superamento di un approccio esegetico fondato sull'interpretazione letterale, evidenziando la necessità di leggere il problema di tutela alla luce di un criterio di ragionevolezza (Figorilli 2002, p. 297 ss.). La medesima dottrina osservava altresì, sulla scorta dei lavori parlamentari, che probabilmente la soluzione migliore per far sì che il giudice potesse pronunciarsi su un provvedimento amministrativo che non rilevasse direttamente nella controversia fosse di ricorrere alla disapplicazione (*ibidem*). Il problema è da ritenersi definitivamente superato in ragione del fatto che ora la normativa prevede espressamente che i limiti interni non si applichino anche rispetto all'intervento sui provvedimenti dell'amministrazione titolare o responsabile.

44. È previsto infatti un doppio canale giurisdizionale, in modo da consentire a chi agisce in giudizio di scegliere se ottenere tutela direttamente in sede giurisdizionale a fronte di una violazione della disciplina in materia di protezione dei dati personali (tutela immediata) oppure se rivolgersi previamente al Garante e poi contestare la decisione del Garante dinanzi al giudice ordinario (tutela avverso i provvedimenti del Garante, ivi inclusi quelli sanzionatori).

45. Cfr. Costantino 2004, p. 1230-1231, il quale pronosticava, sulla base dell'esperienza pregressa, che le controversie emerse in sede di giudizio immediato fossero sostanzialmente marginali.

46. Come noto, ai sensi dell'art. 10, co. 6, d.lgs. n. 150/2011, come modificato dall'art. 17, d.lgs. n. 101/2018, in caso di giudizio immediato, deve procedersi alla notifica del ricorso al Garante per la protezione dei dati (che può eventualmente decidere di intervenire). Nell'ambito della sua attività di redazione di relazioni sulla propria attività a cadenza annuale, il Garante dà conto delle notifiche ricevute nell'ambito di giudizi. Come si evince dalla Relazione del Garante del 2021, p. 204-205, nel 2021 il Garante ha registrato 115 opposizioni, a fronte della notifica di 58 ricorsi e nel 2020 171 opposizioni, a fronte di 56 ricorsi notificati.

47. Sui caratteri, in generale, del giudizio di opposizione a sanzione cfr. Cimini 2017, p. 421 ss.; con particolare riguardo alla materia della privacy, si v. De Rosa 2021, p. 1052 ss.

dal Garante stesso (che, eventualmente, avrà già disposto limitazioni nei confronti del trattamento della pubblica amministrazione)[48].

Più interessante sarebbe valutare come il giudice possa decidere a fronte di situazioni più problematiche, in cui occorre verificare in che misura l'amministrazione abbia fruito dei propri margini di scelta rispetto al trattamento di dati personali operato nell'interesse pubblico. Si pensi ad un trattamento svolto nell'interesse pubblico, perché strumentale ad un determinato procedimento amministrativo. Se la raccolta dei dati personali nell'ambito di tale trattamento è svolta sulla base di un atto amministrativo generale che disciplini diversi trattamenti – fra cui quello qui considerato, e che sia adottato ai sensi dell'art. 2-*ter* Codice privacy – il giudice potrebbe trovarsi nella situazione di poter modificare o revocare siffatto atto, ma ciò richiederebbe di inserirsi in una valutazione assai critica rispetto a come tale atto sia strumentale alla tutela dei dati personali, tenendo conto sia del diritto alla protezione delle persone fisiche sia della necessità di perseguire l'interesse pubblico[49].

3.4. Il giudice ordinario e la responsabilità

Sempre al fine di verificare la misura della tutela garantita dal sistema di tutela giurisdizionale del giudice ordinario rispetto alle violazioni in materia di protezione di dati personali nei trattamenti in ambito pubblico è opportuno esaminare il tema della responsabilità da illecito trattamento dei dati.

L'art. 82 GDPR, recante la disciplina uniforme di tale responsabilità, presenta profili di ambiguità. Per un verso, esso delinea una disciplina senz'altro autosufficiente della responsabilità da illecito trattamento dei dati, giacché consente di individuare tutti gli elementi del fatto illecito, in particolare i soggetti attivi, la condotta, le regole relative all'imputabilità del danno[50]. Così, la responsabilità è attribuita al titolare o al responsabile del trattamento per una condotta che si sia concretata nella violazione del GDPR o di altra norma anche sul piano nazionale relativa alla protezione dei dati, sempreché il soggetto attivo non dimostri che "l'evento dannoso non gli è in alcun modo imputabile"[51]. Per altro verso, la disciplina del GDPR non sembra differenziarsi molto da quella previgente. Nella vigenza dell'ormai abrogato art. 15 del Codice privacy, infatti, il dettato positivo prevedeva l'applicazione alla responsabilità da illecito trattamento dell'art. 2050 c.c. in tema di responsabilità da attività pericolosa[52], anche nel caso di pubbliche amministrazioni titolari o responsabili del trattamento[53]. Ciò equivaleva a dire che la responsabilità

48. Spesso, infatti, il giudice, rigettata l'opposizione, conferma i provvedimenti del Garante. Cfr. in tal senso Trib. Catania, sez. III, 8 luglio 2021, n. 3095, in *Banca dati Merito* (conferma dell'ordinanza-ingiunzione del Garante ad un Comune per la pubblicazione di una delibera recante dati sensibili sul sito web istituzionale); Tribunale di Sciacca del 6 giugno 2016, n. 308, in *Relazione Garante 2020*, p. 210 (conferma della sanzione del Garante ad un Comune per aver illecitamente pubblicato sul sito web istituzionale alcune ordinanze con cui venivano disposti trattamenti sanitari obbligatori); Trib. Taranto, 25 luglio 2019, n. 2553, in *Relazione Garante 2019*, p. 178 (conferma della sanzione del Garante ad un istituto scolastico per mancata informativa e notificazione rispetto a trattamento di dati biometrici dei dipendenti a titolo di sperimentazione per accertarne la presenza sul luogo di lavoro).
49. In un simile caso, inoltre, sarebbe difficile valutare se effettivamente si sia di fronte ad una violazione dei dati personali o se, invece, il *petitum* sostanziale non porti a ritenere radicata la giurisdizione del giudice amministrativo, nella misura in cui la posizione fatta valere da chi agisce in giudizio sia strumentale a far valere l'illegittimità dell'atto più che la lesione della privacy.
50. In questo senso cfr. anche Camardi 2020, p. 802.
51. Così, secondo l'art. 82, par. 3 GDPR.
52. Benché si tenda, sulla base del richiamo all'art. 2050 c.c., a ritenere che l'attività di trattamento fosse qualificabile come attività pericolosa, non va trascurata la tesi fatta propria da Franzoni 2010 p. 676 secondo cui il richiamo all'art. 2050 c.c. servirebbe solamente a richiamare il regime della prova liberatoria di questa responsabilità, senza assimilare il trattamento dei dati ad attività pericolosa.
53. Nonostante in passato si negasse l'applicabilità della responsabilità *ex* art. 2050 c.c. alle pubbliche amministrazioni sulla scorta di una serie di argomenti (si considerino gli argomenti riportati e contestati in Casetta 1956,

da illecito trattamento prevedeva un criterio di imputazione tale per cui il danneggiante si sarebbe liberato della presunzione di responsabilità solo dimostrando la sussistenza di cause esterne alla propria sfera di controllo e, dunque, di caso fortuito[54]. Si è pertanto ritenuto che anche nella casistica relativa alla responsabilità da illecito trattamento dei dati sotto la vigenza del GDPR non vi dovrebbe essere una significativa cesura rispetto al precedente orientamento applicativo fondato sull'art. 2050 c.c.[55]

Ciò posto, sembra che il vero punto dirimente per segnare uno iato con la disciplina precedente non sia tanto il rapporto tra l'art. 82 GDPR e la disciplina in tema di illecito, quanto il rapporto tra l'art. 82 GDPR e i principi in esso contenuti e, in particolare, il principio di *accountability*.

Nella precedente disciplina, fondata sull'art. 2050 c.c. e, dunque, su di una responsabilità interpretata in senso semi-oggettivo[56], il danneggiante, come già rilevato, era liberato solo provando il caso fortuito.

Nella disciplina del GDPR non si ha una regola precisa sulla natura della prova liberatoria[57]: il criterio di imputazione non pare lasciare spazio a valutazioni relative all'elemento soggettivo[58], ma bisogna considerare che l'attribuzione della responsabilità non può che rappresentare il rovescio della medaglia del principio di *accountability*, vero e proprio architrave del GDPR. Detto diversamente, qualora in ottemperanza al predetto principio il titolare (o il responsabile) del trattamento dimostri di aver adottato le misure organizzative e di sicurezza adeguate a contenere il rischio, non dovrebbe essergli imputata alcuna responsabilità. È infatti chiaro che, diversamente opinando, si rischierebbe di rendere pressoché privo di rilievo – sul fronte della responsabilità *ex post* – l'intervento sul piano organizzativo necessario al fine di adeguarsi alle regole sulla protezione dei dati. In effetti, permarrebbe una (vasta) zona grigia in cui, nonostante le misure attuate dal titolare (o responsabile), questi non potrebbe escludere l'imputazione di una violazione che non sarebbe stata evitabile, indipendentemente dall'intervento organizzativo adottato[59]. Il punto è particolarmente rilevante proprio per le pubbliche amministrazioni: tali soggetti trattano infatti dati personali non tanto (o almeno non

p. 890 ss.), una simile eccezione non è stata sollevata per negare la soggezione delle pubbliche amministrazioni titolari/responsabili alle regole relative alla responsabilità da illecito trattamento dei dati. Ne sono testimonianza, da un lato, le pronunce in cui la pubblica amministrazione è stata condannata a risarcire il danno da essa cagionato a causa di illecito trattamento di dati personali (a titolo esemplificativo, si veda Cass. civ., sez. I, 13 maggio 2015, n. 9785) e, dall'altro lato, il fatto che si fosse scelto il richiamo all'art. 2050 c.c. proprio perché non presentava ostacoli la sua applicazione alla pubblica amministrazione (cfr. sul punto Sica 1997, p. 186). Ad ogni modo, come anche attestato in Avanzini 2010, nota 11, il superamento dell'impostazione preclusiva dell'estensione della responsabilità *ex* art. 2050 c.c. alla pubblica amministrazione si è avuto già negli anni Ottanta con Cass., sez. III, 27 gennaio 1982, n. 537, annotata da Alpa 1982, p. 919-920.

54. Cfr. Sica 1997, p. 250 ss. In generale, per questa interpretazione dell'art. 2050 c.c., cfr. Franzoni 2010, p. 440 ss.; Monateri 2001, p. 380 ss.; più recentemente, Trimarchi 2021, p. 430 ss. Si osserva che il riferimento dell'art. 15 Codice privacy è stato inteso come riguardante l'intera "vita" dell'art. 2050, compresa l'interpretazione ad opera delle corti (ed è tale interpretazione che si è radicata in senso semi-oggettivo). In questo senso, si v. Bilotta 2019, p. 445 ss.
55. In questi termini, Mazza 2021, p. 966; Sica 2021, p. 893.
56. Si v. Sica 1997, p. 182.
57. Cfr. Ratti 2019, p. 789.
58. Si nota peraltro che rispetto all'irrogazione delle sanzioni la giurisprudenza eurounitaria ha riconosciuto, sulla base di indici positivi ricavabili dal GDPR, che vada accertato l'elemento soggettivo della sanzione. Si tratta della sentenza Corte di Giustizia Ue, Grande Sezione, 5 dicembre 2023, causa C-683/21, *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos c. Valstybinė duomenų apsaugos inspekcija*. Per un inquadramento di tale profilo sia consentito rinviare a Franca 2024.
59. Il punto pare ben espresso da Bilotta 2019, p. 462 (condivisibilmente l'A. mette in rilievo il ruolo del principio di *accountability*, anche se la natura della responsabilità *de qua* viene qualificata come contrattuale).

solo) per trarne un vantaggio, ma per ottemperare di regola ad obblighi di legge o per l'esecuzione di compiti a rilevanza pubblicistica. In questo senso, sobbarcare l'amministrazione del costo legato a rischi non riconducibili alla propria sfera di controllo si traduce in una significativa svalutazione del fine di interesse pubblico che essa persegue e per cui tratta i dati, anche considerando che tali rischi sono in ultima analisi affrontati per finalità di utilità collettiva.

Un altro punto particolarmente rilevante attiene alla prova del danno. Si era infatti posto il dubbio che, giusto l'utilizzo di termini come danno materiale e immateriale nell'art 82 GDPR – termini non propriamente convergenti rispetto a quelli propri della tradizione giuridica italiana – il regolamento sembrasse fare riferimento ad un danno-conseguenza, dal momento che la divisione danno materiale/immateriale va letta come danno patrimoniale/non patrimoniale[60]. In questi termini, non era tuttavia chiaro se la mera violazione determinasse già un danno (danno *in re ipsa*) oppure se tale danno dovesse essere oggetto di prova da parte del danneggiato[61].

Il punto è stato risolto dalla giurisprudenza della Corte di giustizia, la quale ha in più circostanze affermato che non è sufficiente addurre la violazione delle norme in materia di protezione dei dati personali per avere diritto al risarcimento, essendo altresì necessario dare prova del danno[62].

D'altronde, la configurazione di un danno *in re ipsa* si porrebbe in contrasto con il *proprium* dell'attività amministrativa di trattamento dei dati personali, caratterizzata dal fatto di essere strumentale non solo alla tutela dei soggetti interessati, ma anche alla libera circolazione dei loro dati, *sub specie* di interesse pubblico. Se al mero sorgere di una violazione si riconosce infatti un diritto al risarcimento – inteso in prospettiva essenzialmente sanzionatoria – perde di riferimento la circostanza che tale attività è funzionale non solo alla tutela del singolo, ma anche a favorire la libera circolazione dei dati personali di quest'ultimo[63].

Il rischio è che una siffatta lettura possa dunque ostacolare lo svolgimento dell'attività di trattamento dei dati personali e possa condurre la pubblica amministrazione ad un atteggiamento essenzialmente inerte, secondo logiche di burocrazia difensiva[64]. In tal modo, dunque, l'eccessiva – in quanto travalicante la logica riparativa – salvaguardia del diritto alla protezione dei dati come diritto di "esclusione", finirebbe col pregiudicare lo

60. In questa prospettiva si v. Ratti 2019, p. 774; Riccio 2022, p. 726; Tosi 2020, p. 1133.

61. Si tratta di una questione non nuova rispetto all'illecito trattamento di dati personali che poteva dirsi sostanzialmente risolta nel vigore della vecchia disciplina. L'impostazione del danno *in re ipsa*, a livello giurisprudenziale e per quanto riguarda la disciplina del previgente Codice privacy, è stata seguita da alcune pronunce di merito e recisamente respinta dalla Suprema Corte (cfr., Cass. civ., sez. I, 10 giugno 2021, n. 16402; Cass. civ., sez. VI, 12 novembre 2019, n. 29206; Cass. civ., sez. VI, 18 luglio 2019, n. 19434).

62. Cfr., anzitutto, Corte di Giustizia Ue, III Sezione, 4 maggio 2023, causa C-300/21, UI c. *Österreichische Post AG*, la quale ha stabilito che "la mera violazione delle disposizioni di tale regolamento non è sufficiente per conferire un diritto al risarcimento" (in tema cfr. Navone 2024, p. 415 ss. Alonzo 2023, p. 1971 ss.). Più recentemente si v. anche Corte di Giustizia Ue, III Sezione, 20 giugno 2024, cause riunite C182/22 e C189/22, *JU (C182/22), SO (C189/22) c. Scalable Capital GmbH* in cui si specifica altresì la funzione compensativa della responsabilità *ex* art. 82 GDPR e si offrono alcuni chiarimenti rispetto alla nozione di danno immateriale, rilevando, ad esempio, che esso non ha di per sé natura meno grave di una lesione personale.

63. Si tratta dunque di non trascurare la forte vena mercantilistica, fondata sulla libera circolazione dei dati, pur senza considerare essa come sovrastante l'esigenza di protezione della persona. Il punto è ben sviluppato in Camardi 2020, p. 803 ss.

64. Sul fenomeno della burocrazia difensiva si v., in part., Battaglia–Battini–Blasini et al. 2021, p. 1295 ss.; Bottino 2020, p. 117 ss.; Cafagno 2018, p. 625 ss.; Giomi 2021-b, p. 663 ss.; Lorenzoni 2021, p. 761 ss. È pur vero che, come si vedrà *infra*, il funzionario risponderà solo a titolo di dolo o colpa grave. Cionondimeno, l'incertezza legata all'individuazione di ipotesi di colpa grave potrebbe attivare meccanismi di burocrazia difensiva.

stesso diritto alla protezione dei dati, inteso come funzionale alla libera circolazione dei dati.

3.4.1. Le ripercussioni in termini di responsabilità erariale

Nella misura in cui l'amministrazione è destinataria di una condanna risarcitoria rispetto al danno causato dall'illecito trattamento di dati oppure di un atto sanzionatorio del Garante, si ha un accertamento rispettivamente in via giudiziale o in via amministrativa della violazione avvenuta. In entrambi i casi, l'accertamento operato – con contestuale pronuncia di condanna, nell'un caso, o provvedimento sanzionatorio, nell'altro caso – ha ad oggetto l'avvenuta violazione di una regola in materia di protezione dei dati personali da parte del titolare o responsabile del trattamento. Ciò significa che, per quanto riguarda le persone giuridiche titolari o responsabili del trattamento, saranno queste a rispondere del pregiudizio patrimoniale pagando la sanzione, ovvero risarcendo il danno. Si realizza, dunque, nelle due ipotesi un illecito trattamento capace di generare diverse poste di danno risarcibile. Vi sono infatti fattispecie in cui altri soggetti "esterni", siano essi contitolari o responsabili del trattamento, sono chiamati a rispondere del danno risarcibile in via solidale. In questo caso, il Regolamento europeo prevede espressamente un regime di solidarietà passiva di tali soggetti rispetto al risarcimento del danno[65].

Più complesso risulta il profilo riguardante il riparto della responsabilità fra i soggetti facenti parte della struttura organizzativa. Il quadro organizzativo della pubblica amministrazione dal punto di vista della protezione dei dati può prevedere diverse figure soggettive, ossia il Responsabile della protezione dei dati, eventuali responsabili interni e i soggetti autorizzati al trattamento.

A tale riguardo, è stato rilevato che la disciplina eurounitaria della responsabilità civile circoscriverebbe il novero dei legittimati passivi ai soli titolari e responsabili: in questi termini, i soggetti incaricati del trattamento e i responsabili interni non ricadrebbero entro lo spettro applicativo della norma risarcitoria e sarebbero responsabili solo ai sensi delle norme risarcitorie di diritto comune[66]. Si tratta di una circostanza che non sembra compatibile con il principio di *accountability*, almeno se lo si legge come responsabilizzazione dell'organizzazione che coinvolge anche le sue ramificazioni, non solo l'organizzazione generalmente intesa.

Ad ogni buon conto, nel caso di trattamento in ambito pubblico e per quanto riguarda i danni relativi alla protezione dei dati e le *deminutiones* legate all'irrogazione di sanzioni da parte del Garante, è da ritenere sussistente la responsabilità amministrativa del funzionario. In questi termini, dunque, la condanna dell'amministrazione non esclude – e anzi comporta – che il funzionario, sussistendone i presupposti, sia chiamato a rispondere del danno erariale arrecato all'amministrazione in sede contabile. Rispetto a quanto può avvenire con riferimento ad organizzazioni private, tuttavia, non va trascurato un profilo di specialità dell'amministrazione, dato dal fatto che il funzionario risponde unicamente per colpa grave[67].

Si tratta di un compromesso (reso necessario dall'intreccio tra norme relative alla protezione dei dati e norme che disciplinano la responsabilità dei funzionari) che appare più coerente rispetto ad un esonero di responsabilità di responsabili interni e autorizzati al trattamento.

Se infatti si applicasse rigidamente la tesi della responsabilità della sola organizzazione e, nella specie, dell'amministrazione, ciò si tradurrebbe in una sostanziale deresponsabilizzazione dei funzionari che operano in essa e che, a certe

65. Cfr. quanto previsto dall'art. 82, par. 4 GDPR.

66. Per questa prospettazione cfr. Thobani 2019, p. 1226; *contra* Policella 2019, p. 443.

67. Si possono pertanto immaginare ipotesi in cui la colpa lieve che ha portato, ad esempio, ad una condanna per illecito trattamento, non superando la soglia della colpa grave, non è imputabile al funzionario e, dunque, permane come colpa dell'organizzazione. Ciò evidentemente non rappresenta una novità, ma la mera conseguenza della limitazione della responsabilità del funzionario al dolo e alla colpa grave. Non va trascurato, inoltre, che l'indagine relativa alla sussistenza della colpa grave è resa piuttosto incerta dal fatto di essere individuata, in assenza di tipizzazione, su base eminentemente pretoria. Sul problema della (mancata) tipizzazione della colpa grave e sul suo legame con il fenomeno della burocrazia difensiva cfr. Cimini–Valentini 2022, p. 10 ss.; Spasiano 2021, spec. p. 301.

condizioni, una volta istruiti e autorizzati, assumono un ruolo di responsabilità nella filiera di trattamento del dato.

In questa prospettiva, si potrebbe pensare che la "delega" di compiti relativi alla protezione dei dati personali a specifici soggetti all'interno dell'organizzazione possa consentire al rappresentante (persona fisica) del titolare di andare esente da responsabilità. È quanto è accaduto in un caso recente deciso dalla Corte dei Conti di Bolzano[68] in cui si è ritenuto che il privacy manager fosse il soggetto unicamente responsabile per le violazioni compiute sul piano della protezione dei dati, mantenendo esente il rappresentante legale dell'ente titolare del trattamento.

Orbene, al netto del fatto che spetta al titolare anche individuare in modo circostanziato le competenze in materia di protezione dei dati personali[69], l'impostazione della corte bolzanina non pare condivisibile in base alla previgente disciplina in tema di protezione dei dati personali[70] e, a maggior ragione, in un sistema fondato sul principio di *accountability*. Fermo restando che, in un sistema organizzativo governato da tale principio, non è ammissibile che a rispondere sia solo il rappresentante del titolare.

La riflessione sin qui condotta consente, altresì, di svolgere una considerazione ulteriore che si lega alla enucleazione di un'attività di trattamento dei dati personali.

Lo svolgimento di tale attività, infatti, consente di offrire al giudice contabile il tracciato del percorso decisionale seguito dall'amministrazione: percorso che, evidentemente, include anche gli snodi attraverso i diversi soggetti intervenuti sul trattamento dei dati e sull'organizzazione del medesimo.

Ancorando la valutazione del giudice contabile a detto percorso decisionale[71], sembra dunque possibile non solo giustificare quanto sinora rilevato in termini di responsabilità amministrativa anche dei responsabili interni e degli autorizzati al trattamento, ma anche definire un parametro attraverso cui individuare e graduare la loro responsabilità, evitando ipotesi sia di deresponsabilizzazione che di eccessiva responsabilizzazione[72].

4. Considerazioni conclusive

L'analisi svolta ha permesso di porre in luce come la tutela in materia di protezione dei dati personali, quando rapportata ai trattamenti operati nell'interesse pubblico, presenti tratti peculiari che la distinguono dal regime dei trattamenti svolti in ambito privato.

Tenendo conto del fatto che il diritto alla protezione dei dati personali non si esaurisce in una concezione meramente difensiva, ma incorpora in modo strutturale anche la dimensione della libera circolazione dei dati si coglie questa duplice natura nel contesto pubblico. Essa si traduce nella costante tensione tra esigenze di protezione della persona

68. Cfr. Corte conti, sez. Bolzano, 9 gennaio 2024, n. 1.

69. Come si evince da Corte conti, sez. giur. Calabria, 8 novembre 2019, n. 429. Con deliberazione della giunta regionale calabrese, la funzione di "tutela della privacy" era stata assegnata al Servizio II del *Dipartimento Bilancio e patrimonio*, unitamente alla funzione di vigilanza sulla sicurezza sui luoghi di lavoro. La Corte, oltre a rilevare l'attribuzione della funzione di tutela della privacy in modo promiscuo ad altre, soggiunge che nel caso in esame "difetta infatti l'esistenza di un atto scritto indirizzato al responsabile nominato, così come la puntuale individuazione delle competenze specifiche dell'interessato e la corretta delimitazione dei suoi poteri, nonché quell'esercizio costante di poteri di vigilanza e di istruzione previsto dalla conferente normativa".

70. Si consideri, infatti, che, a mente della previgente disciplina, responsabili interni e incaricati al trattamento erano pacificamente ritenuti corresponsabili assieme al titolare. Cfr. in tema Comandè 2007, p. 393 ss.; Roppo 1997, p. 661.

71. Si allude all'impostazione di Giomi 2021-a, p. 365 ss. che mette in luce la rilevanza del momento della decisione, come fattore di ausilio per il giudice contabile rispetto all'individuazione corretta della responsabilità erariale.

72. In una lettura rigida della normativa in materia di protezione dei dati, infatti, si rischia di attribuire una responsabilità particolarmente ampia ai soggetti apicali di ciascuna organizzazione. Questi hanno sicuramente un alto grado di responsabilità nella definizione di misure adeguate in tema di protezione dei dati, ma non può ricadere su costoro, in ogni situazione, l'integralità del danno legato ad un concorso fra colpe.

ed esigenze di efficienza ed efficacia dell'azione amministrativa, entrambe pienamente ancorate al dettato costituzionale e supportate da un quadro assiologico di riferimento.

In questa linea ricostruttiva, la tutela amministrativa affidata al Garante mostra alcune criticità. L'Autorità tende a valorizzare soprattutto la conformità formale dei trattamenti con il rischio di trascurare un equilibrato bilanciamento con l'interesse pubblico sottostante. Come dimostrano i casi esaminati (dal "bonus Covid" alla profilazione sanitaria emergenziale), la rigidità nell'applicazione dei principi del trattamento può condurre a esiti sproporzionati, che sacrificano indebitamente le finalità pubblicistiche per garantire una tutela (invero solo astratta, in alcuni casi) dell'interessato. Se è vero che il sistema di protezione non subordina la rilevanza delle violazioni a un danno effettivo, è altrettanto vero che l'interpretazione dei principi non può essere sganciata dal contesto in cui il trattamento avviene, pena il rischio di concepire la protezione dei dati come un diritto a soddisfazione necessaria e in quanto tale prevalente su qualsiasi altra posizione radicata sul trattamento.

Sul versante giurisdizionale, l'attribuzione di una giurisdizione esclusiva al giudice ordinario rappresenta una scelta singolare e non priva di criticità. Essa, da un lato, garantisce (o dovrebbe garantire?) una giurisdizione piena, con la possibilità per il giudice di modificare o revocare provvedimenti amministrativi e di condannare al risarcimento del danno. Dall'altro, però, pone problemi in termini di effettività della tutela. Ciò emerge particolarmente se si rapporta il modello del sindacato del giudice ordinario a quello del giudice amministrativo, tradizionalmente esperto nel bilanciamento tra interessi pubblici e privati: la minore propensione del giudice ordinario a seguire questa impostazione rischia di limitare la capacità del sistema di affrontare adeguatamente i casi più complessi. A ciò si aggiunge la non appellabilità delle decisioni di primo grado, che riduce le garanzie di effettività della tutela nella misura in cui, non consentendo un giudizio di appello vero e proprio, rischia di creare alcune incomprensioni derivanti dalla complessità fattuale sottesa almeno ad alcuni trattamenti di dati personali.

Infine, il profilo risarcitorio apre ulteriori interrogativi. L'applicazione del principio di *accountability* dovrebbe consentire di perimetrare la responsabilità sia sul piano del danno da illecito trattamento che rispetto alle conseguenze sul fronte erariale.

Se il superamento della tesi del danno da illecito trattamento come danno *in re ipsa* pare favorire una logica compatibile con questa impostazione, pare invece che sul fronte della responsabilità erariale la giurisprudenza mostri alcune incertezze che sembrano sottendere, ancora una volta, una logica formalistica nell'attribuzione della responsabilità.

Nel loro insieme, questi elementi inducono a ritenere che il sistema attuale rischi di mostrare fragilità laddove si tratta di valutare la conformità al GDPR di trattamenti funzionali all'esercizio della funzione amministrativa. È dunque necessario un processo di adattamento che, da un lato, eviti di ridurre la tutela a un controllo meramente formale e, dall'altro, valorizzi l'esigenza circolatoria incarnata dal perseguimento dell'interesse pubblico. In prospettiva, ciò richiederà una sempre maggiore integrazione tra principi della protezione dei dati e principi tipici del diritto amministrativo. Come si è visto, infatti, un correttivo – rispetto a letture particolarmente critiche della disciplina di protezione dei dati personali nell'esercizio delle diverse funzioni di tutela amministrativa e giurisdizionale – riposa nella lettura dei principi del GDPR alla luce dei principi dell'azione amministrazione: ad esempio, leggendo la minimizzazione come necessarietà del trattamento dei dati rispetto ad un'azione efficace da parte dell'amministrazione. In conclusione, tramite questo approccio sembra possibile garantire un sistema di tutele realmente equilibrato, capace di proteggere le persone cui i dati si riferiscono senza indebolire la capacità delle istituzioni di perseguire le finalità a esse attribuite dalla legge.

Riferimenti bibliografici

E. Alonzo (2023), *La risarcibilità del danno "bagatellare" in materia di violazioni della normativa GDPR*, in "Responsabilità civile e previdenza", 2023, n. 6

G. Alpa (1982), *Attività pericolosa e responsabilità dell'ENEL. Verso l'erosione dei privilegi della pubblica amministrazione?*, in "Giustizia civile", 1982, n. 1

S. Amorosino (2004), *Tipologie e funzioni delle vigilanze pubbliche sulle attività economiche*, in E. Bani, M. Giusti (a cura di), "Vigilanze economiche. Le regole e gli effetti", Cedam, 2004

M. Antonioli (2013), *Vigilanza e vigilanze tra funzione e organizzazione*, in "Rivista trimestrale di diritto pubblico", 2013, n. 3

G. Avanzini (2010), *Nuovi sviluppi nella responsabilità delle amministrazioni per danni derivanti da attività pericolose e da cose in custodia*, in "Diritto amministrativo", 2010, n. 1

A. Battaglia, S. Battini, A. Blasini et al. (2021), *"Burocrazia difensiva": cause, indicatori e rimedi*, in "Rivista trimestrale di diritto pubblico", 2021, n. 4

F. Bilotta (2019), *La responsabilità civile nel trattamento dei dati personali*, in R. Panetta (a cura di), "Circolazione e protezione dei dati personali tra libertà e regole del mercato", Giuffrè, 2019

M. Bombardelli (2022), voce *Dati personali (tutela dei)*, in "Enciclopedia del diritto. I tematici", III, Giuffrè, 2022

G. Bottino (2020), *La burocrazia «difensiva» e le responsabilità degli amministratori e dei dipendenti pubblici*, in "Analisi Giuridica dell'Economia", 2020, n. 1

F. Bravo (2018), *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Wolters Kluwer, 2018

E. Bruti Liberati (2019), *La regolazione indipendente dei mercati. Tecnica, politica e democrazia*, Giappichelli, 2019

M. Cafagno (2018), *Contratti pubblici, responsabilità amministrativa e "burocrazia difensiva"*, in "Il diritto dell'economia", 2018, n. 3

V. Caianiello (1997), *Le autorità indipendenti tra potere politico e società civile*, in "Foro amministrativo", 1997, n. 2

C. Camardi (2020), *Note critiche in tema di danno da illecito trattamento dei dati personali*, in "Jus civile", 2020, n. 3

M.T.P. Caputi Jambrenghi (2017), *La funzione amministrativa neutrale*, Cacucci, 2017

F. Cardarelli (2021), *sub Artt. 60-62 GDPR*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), "Codice della privacy e data protection", Giuffrè, 2021

E. Carloni (2022), *Il paradigma trasparenza. Amministrazioni, informazione, democrazia*, il Mulino, 2022

E. Casetta (1956), *Gli enti pubblici e l'art. 2050 c.c.*, in "Giurisprudenza italiana", 1956, n. 1

P. Cerbo (2012), *Giudice ordinario e "sostituzione" della pubblica amministrazione*, in "Rivista trimestrale di diritto e procedura civile", 2012, n. 3

A. Chizzini (2018), *La tutela giurisdizionale dei diritti*, Giuffrè, 2018

S. Cimini (2017), *Il potere sanzionatorio delle amministrazioni pubbliche. Uno studio critico*, Editoriale Scientifica, 2017

S. Cimini, F. Valentini (2022), *La dubbia efficacia dello "scudo erariale" come strumento di tutela del buon andamento della p.a.*, in "Ambientediritto.it", 2022, n. 1

M. Clarich (1997), *Privacy informatica: osservazioni*, in "Danno e responsabilità", 1997, n. 2

G. Comandè (2007), *sub art. 15*, in C.M. Bianca, F.D. Busnelli (a cura di), "La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 ("Codice della privacy")", I, Cedam, 2007

G. Costantino (2004), *La tutela giurisdizionale dei diritti al trattamento dei dati personali*, in "Rivista trimestrale di diritto e procedura civile", 2004, n. 4

M. De Bellis (2021), *I poteri ispettivi dell'amministrazione europea*, Giappichelli, 2021

M. De Donno (2019), *La tutela del controinteressato nell'accesso civico generalizzato*, in G. Gardini, M. Magri (a cura di), "Il FOIA italiano: vincitori e vinti. Un bilancio a tre anni dall'introduzione", Maggioli, 2019

M. De Rosa (2021), *Il procedimento sanzionatorio presso il garante per la tutela dei dati personali: cosa cambia alla luce delle norme europee e del nuovo codice*, in A. Cagnazzo, S. Toschei, F. Tuccari (a cura di), "La vigilanza e la procedura di irrogazione delle sanzioni amministrative", Giuffrè, 2021

G. Della Cananea (2005), *Regolazione del mercato e tutela della concorrenza nella risoluzione delle controversie in tema di comunicazioni elettroniche*, in "Diritto pubblico", 2005, n. 2

A. Di Majo (1992), *Tutela (dir. priv.)*, in "Enciclopedia del diritto", vol. XLV, Giuffrè, 1992

G. Falcon (2015), *Conclusioni*, in G. Falcon, B. Marchetti (a cura di), "Verso nuovi rimedi amministrativi? Modelli giustiziali a confronto", Editoriale Scientifica, 2015

S. Faro (2000), *Trattamento dei dati personali e tutela della persona*, in "Digesto delle discipline pubblicistiche, Aggiornamento", Utet, 2000

L. Ferola (2019), *sub art. 6o GDPR*, in A. Barba, S. Pagliantini (a cura di), "Commentario del codice civile. Leggi collegate. II", Utet, 2019

F. Figorilli (2002), *Giurisdizione piena del giudice ordinario e attività della pubblica amministrazione*, Giappichelli, 2002

S. Franca (2024), *Il regime del trattamento di dati personali: persistenti incertezze e nuovi capisaldi*, in "Giornale di diritto amministrativo", 2024, n. 3

S. Franca (2023), *I dati personali nell'amministrazione pubblica. Attività di trattamento e tutela del privato*, Editoriale Scientifica, 2023

F. Francario (2023), *Il trattamento dei dati personali per finalità di pubblico interesse e l'auspicio di un mutamento di indirizzo*, in "Giustiziainsieme.it", 2023

F. Francario (2022), *Il trattamento dei dati personali per finalità di pubblico interesse*, in "Giustiziainsieme.it", 2022

M. Franzoni (2010), *L'illecito*. I, Giuffrè, 2010

G. Gardini (2024), *Le regole dell'informazione. Pluralismo e libertà nell'era dell'intelligenza artificiale*, Giappichelli, 2024

E. Giannantonio (1999), *Dati personali (tutela dei)*, in "Enciclopedia del diritto", Agg. III, Giuffrè, 1999

V. Giomi (2021-a), *Processo contabile e decisione amministrativa: le dinamiche di una relazione complessa*, in "Diritto processuale amministrativo", 2021, n. 2

V. Giomi (2021-b), *Giudice contabile e decisione amministrativa di transigere: fra burocrazia difensiva e rischi percepiti*, in "Nuove Autonomie", 2021, n. 3

M. Gola (2011), *La giustizia innanzi all'Autorità garante della* privacy, in G. Clemente di San Luca (a cura di), "La tutela delle situazioni soggettive nel diritto italiano, europeo e comparato. II. La tutela delle situazioni soggettive nell'amministrazione giustiziale", Editoriale Scientifica, 2011

P. Licci (2011), sub *art. 10 d.lgs. 1º settembre 2011, n. 150*, in B. Sassani, R. Tiscini (a cura di), "La semplificazione dei riti civili", Dike Giuridica, 2011

M. Macchia, C. Figliolia (2018), *Autorità per la privacy e Comitato europeo nel quadro del* General Data Protection Regulation, in "Giornale di diritto amministrativo", 2018, n. 4

F. Lorè (2022), *Il caso "bonus Covid" in favore dei titolari di cariche pubbliche: i rilievi sollevati all'INPS dal Garante per la protezione dati personali*, in "Ammnistrativ@mente", 2022, n. 1

L. Lorenzoni (2021), *La responsabilità amministrativa in relazione al fenomeno della cosiddetta burocrazia difensiva*, in "Il lavoro nelle pubbliche amministrazioni", 2021, n. 4

V. Lubello (2021), sub *Art. 17 d.lgs. 10 agosto 2018, n. 101*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), "Codice della privacy e data protection", Giuffrè, 2021

A. Mantelero (2015), *Rilevanza e tutela della dimensione collettiva della tutela dei dati personali*, in "Contratto e impresa. Europa", 2015, n. 1

P. Mazza (2021), *Profili processuali del diritto alla protezione dei dati personali nel regime del Reg. UE 2016/679 (GDPR) e del riformato D.Lgs. n. 196/2003*, in "Corriere giuridico", 2021, n. 7

F. Merusi (2000), *Democrazia e autorità indipendenti. Un romanzo "quasi" giallo*, il Mulino, 2000

F. Midiri (2019), sub *art. 57 GDPR*, in A. Barba, S. Pagliantini (a cura di), "Commentario del codice civile. Leggi collegate. II", Utet, 2019

F. Midiri (2017), *Il diritto alla protezione dei dati personali. Regolazione e tutela*, Editoriale Scientifica, 2017

P.G. Monateri (2001), *Manuale della responsabilità civile*, Utet, 2001

G. Mulazzani (2019), *Il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di un pubblico potere*, in G. Finocchiaro (a cura di), "La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d. lgs. 10 agosto 2018, n. 101", Zanichelli, 2019

G. Navone (2024), *Il "danno immateriale" da illecito trattamento dei dati personali*, in "Studi senesi", 2024, n. 2

I. Pagni (2012), sub *art. 10 d.lgs. 1º settembre 2011, n. 150*, in C. Consolo (a cura di), "Codice di procedura civile commentato. La "semplificazione" dei riti e le altre riforme processuali 2010-2011", Ipsoa, 2012

E. Pelino (2019), sub *art. 10 d.lgs. 150/2011*, in L. Bolognini, E. Pelino (a cura di) (2019), "Codice della disciplina privacy", Giuffrè, 2019

R. Perez (1996), *Autorità indipendenti e tutela dei diritti*, in "Rivista trimestrale di diritto pubblico", 1996, n. 1

I. Piazza (2021), *Strumentalità dell'accesso difensivo e sindacato giurisdizionale (nota a Cons. Stato, sez. III, 31 dicembre 2020, n. 8543)*, in "Giustiziainsieme.it", 2021

M. Pietrangelo (2020), *Il linguaggio giuridico-istituzionale sul web e la disinformazione pubblica online*, in "federalismi.it", 2020, n. 11

M. Pietrangelo (2007), *La società dell'informazione tra realtà e norma*, Giuffrè, 2007

O.E. Policella (2019), sub *art. 82*, in L. Bolognini, E. Pelino (a cura di) (2019), "Codice della disciplina privacy", Giuffrè, 2019

A. Principato (2015), *Verso nuovi approcci alla tutela della privacy: privacy by design e privacy by default settings*, in "Contratto e impresa. Europa", 2015, n. 1

M. Ratti (2019), *La responsabilità da illecito trattamento dei dati personali*, in G. Finocchiaro (a cura di), "La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 agosto 2018, n. 101", Zanichelli, 2019

G.M. Riccio (2022), sub *art. 82 GDPR*, in G.M. Riccio, G. Scorza, E. Belisario (a cura di), "GDPR e normativa privacy. Commentario", Wolters Kluwer, 2022

V. Ricciuto (2022), *L'equivoco della privacy. Persona* vs *dato personale*, Edizioni Scientifiche Italiane, 2022

V. Roppo (1997), *La responsabilità civile per trattamento di dati personali*, in "Danno e responsabilità", 1997, n. 6

A.M. Sandulli (1964/1990), *Funzioni pubbliche neutrali e giurisdizione*, in "Rivista di diritto processuale", 1964, nonché in Aa.Vv., "Studi in onore di Antonio Segni", Giuffrè, 1967, IV, ora in A.M. Sandulli, "Scritti giuridici. II", Jovene, 1990

A.M. Sandulli (1989), *Manuale di diritto amministrativo*, vol. I-II, Jovene, 1989

M. Savino (2019), *Il FOIA italiano e i suoi critici: per un dibattito scientifico meno platonico*, in "Diritto amministrativo", 2019, n. 3

A. Simonati (2023), *Il trattamento di dati personali e gli accessi amministrativi "generali": le dinamiche frontiere della discrezionalità*, in "Diritto amministrativo", 2023, n. 1

S. Sica (2021), *sub art. 82 GDPR*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), "Codice della privacy e data protection", Giuffrè, 2021

S. Sica (1997), *sub art. 18*, in E. Giannantonio, M.G. Losano, V. Zeno-Zencovich (a cura di), "La tutela dei dati personali. Commentario alla l. 675/1996", Cedam, 1997

M.R. Spasiano (2021), *Riflessioni in tema di nuova (ir)responsabilità erariale e la strada della tipizzazione della colpa grave nella responsabilità erariale dei pubblici funzionari*, in "Diritto processuale amministrativo", 2021, n. 2

M. Stipo (1994), *Vigilanza e tutela (dir. amm.)*, in "Enciclopedia del diritto", Giuffrè, 1994

S. Thobani (2019), *sub art. 82 GDPR*, in A. Barba, S. Pagliantini (a cura di), "Commentario del codice civile. Leggi collegate. II", Utet, 2019

F. Tigano (2022), *Protezione dei dati personali e pubblica amministrazione: alcuni spunti di riflessione*, in "Diritto e società", 2022, n. 2

L. Torchia (1996), *Gli interessi affidati alla cura delle autorità indipendenti*, in S. Cassese, C. Franchini (a cura di), "I garanti delle regole. Le autorità indipendenti", il Mulino, 1996

S. Torricelli (2023), *Autorità indipendenti e (governo della) discrezionalità*, in "Amministrativ@mente", 2023, n. 2

E. Tosi (2020), *Illecito trattamento dei dati personali, responsabilizzazione, responsabilità oggettiva e danno nel GDPR: funzione deterrente-sanzionatoria e rinascita del danno morale soggettivo*, in "Contratto e Impresa", 3, 2020, n. 3

P. Trimarchi (2021), *La responsabilità civile: atti illeciti, rischio, danno*, III ed., Giuffrè, 2021

S. Valentini (1993), *Vigilanza*, in "Enciclopedia del diritto", vol. XLVI, Giuffrè, 1993

G. Vesperini (1990), *Le funzioni delle autorità amministrative indipendenti*, in " Diritto della banca e del mercato finanziario", 1990, n. 4

N. Vettori (2019), *Valori giuridici in conflitto nel regime delle forme di accesso civico*, in "Diritto amministrativo", 3, 2019

L. Zannini (1992), *Tutela (dir. rom.)*, in "Enciclopedia del diritto", vol. XLV, Giuffrè, 1992

N. Zorzi Galgano (2019), *Le due anime del GDPR e la tutela del diritto alla privacy*, in N. Zorzi Galgano (a cura di), "Persona e mercato dei dati. Riflessioni sul GDPR", Cedam, 2019

Sezione monografica

I dati in ambito pubblico tra esercizio della funzione amministrativa e regolazione del mercato

Parte 2 - Trattamento dei dati e regolazione del mercato

a cura di

Marco Bombardelli, Simone Franca, Anna Simonati

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0241 • articolo sottoposto a peer review • pubblicato in anteprima il 28 ott. 2025

Francesco Midiri

Il ruolo delle autorità indipendenti nella regolazione del trattamento dei dati

Lo studio rileva che la normativa in materia di protezione dei dati personali, per il tramite della funzione di regolazione, viene attuata anche al di là del proprio ambito naturale di operatività fino a condizionare l'applicazione di altre discipline dell'ordinamento (quali quelle relative alla concorrenza, alla tutela dei lavoratori ed alla attività amministrativa algoritmica), in considerazione del fatto che essa viene percepita come la forma più adeguata di protezione dei diritti fondamentali nella civiltà digitale. Le autorità di regolazione, peraltro, debbono realizzare questa tendenza secondo un rigido principio di legalità, cioè attuando esclusivamente i compiti attribuiti dal GDPR: proteggere i dati personali garantendo, nel medesimo tempo, la libera circolazione delle informazioni per lo sviluppo economico sociale. Così, ad esempio, dovranno essere colpite le violazioni della *data protection* realmente lesive, cioè in grado di pregiudicare concretamente le libertà fondamentali. In caso contrario, le autorità genereranno una regolazione eccessivamente vincolistica introducendo, nei vari settori dell'ordinamento, regole e sanzioni che il legislatore non ha voluto.

Regolazione – Protezione dei dati personali – Garanzia dei diritti fondamentali – Principio di legalità

The role of independent regulatory authorities in the governance of data processing

The study highlights how *data protection* legislation, through regulatory functions, is being implemented beyond its natural scope, to the point of influencing the application of other legal provisions (such as those relating to competition, worker protection, and algorithmic administrative activity), given that it is perceived as the most appropriate form of protection of fundamental rights in the digital age. Regulatory authorities, however, must implement this trend according to a strict principle of legality, that is, by exclusively carrying out the tasks assigned by the GDPR: protecting personal data while simultaneously ensuring the free flow of information for economic and social development. Thus, for example, *data protection* violations that are truly harmful, i.e., those capable of concretely undermining fundamental freedoms, must be punished. Otherwise, the authorities will create overly restrictive regulation by introducing rules and sanctions in various areas of the legal system that the legislator did not intend.

Regulation – Protection of personal data – Guarantee of fundamental rights – Principle of legality

L'Autore è professore ordinario di Diritto amministrativo e pubblico nell'Università Cattolica del Sacro Cuore di Milano

Questo contributo fa parte della sezione monografica *I dati in ambito pubblico tra esercizio della funzione amministrativa e regolazione del mercato* a cura di Marco Bombardelli, Simone Franca, Anna Simonati

Sommario: 1. L'applicazione della normativa di *data protection* fuori dal proprio ambito naturale di applicabilità ad opera della regolazione. – 2. I casi recenti di applicazione espansiva della *data protection* in differenti ambiti normativi. – 3. Alcune considerazioni sull'ammissibilità di questa vocazione espansiva della normativa e della regolazione di *data protection*.

1. L'applicazione della normativa di *data protection* fuori dal proprio ambito naturale di applicabilità ad opera della regolazione

Per delineare il ruolo delle autorità amministrative indipendenti di *data protection* nella regolazione del trattamento dei dati non bisogna fare riferimento solo alle funzioni attribuite dalle disposizioni del GDPR (General Data protection Regulation, Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016)[1] le quali attribuiscono alle amministrazioni nazionali le competenze classiche di regolazione o di *command and control* (normative, di controllo, di vigilanza e di sanzione). Il tutto con i relativi problemi di "concentrazione" di funzioni di diversa natura in capo a medesimi soggetti pubblici e di "concentrazione" delle normative che le disciplinano[2].

Per cogliere, invece, la nuova *mission* complessiva che queste autorità stanno assumendo occorre considerare la loro tendenza attuale ad applicare la normativa di protezione dei dati personali anche oltre i suoi "naturali" ambiti di operatività. Ciò non significa che queste amministrazioni applichino regole di protezione dei dati personali al di fuori o in assenza del loro ordinario presupposto di applicazione, rappresentato dalla fattispecie di trattamento delle informazioni. Piuttosto, dopo che queste disposizioni sono state chiamate a regolare fenomeni di utilizzo delle informazioni, i Garanti le utilizzano per condizionare l'interpretazione e gli esiti applicativi di altre normative che regolano differenti materie del sistema giuridico, quasi come si trattasse di norme interposte. Il tutto come se le disposizioni di protezione nascessero nel trattamento dei dati ma andassero a morire in campi regolati da altre discipline, di cui condizionano il portato normativo.

Attraverso queste dinamiche la regolazione di *data protection* sta assumento un carattere espansivo, trasversale e totalizzante ed interessa progressivamente, unificandoli, vari settori normativi.

Certamente, questa tendenza è agevolata da alcuni caratteri fondamentali della normativa di protezione dei dati personali.

Innanzitutto, il diritto alla protezione dei dati personali si presenta come una situazione soggettiva formale e strumentale, cioè diretta ad ottenere l'applicazione dei principi e delle forme del GDPR come "strumento" per proteggere altri diritti fondamentali, consolidatisi nella tradizione giuridica europea[3]. Si tratta, quindi, di una pretesa divenuta ad ampio spettro, in grado di garantire posizioni attive diverse di segno culturale, sociale ed economico (dalla libertà di manifestare il proprio pensiero, al diritto all'assistenza sociale, alla possibilità di ottenere un mutuo). Per questo, la regolazione

1. Si tratta dei poteri conferiti dagli artt. 51, 57 e 58 del GDPR su cui sia consentito rinviare a Midiri 2019-a, Midiri 2019-b, Midiri 2019-c.
2. Problemi che la dottrina ha recentemente illustrato, cfr. Vettori 2024, con riferimento alle Autorità che regolano le dinamiche di mercato.
3. Sia consentito rinviare a Midiri 2017.

tende ad applicare questo diritto in maniera onnicomprensiva, in vari ambiti dell'agire umano.

Ancora, il principio di *accountability* (art. 5 GDPR)[4], ma ancora di più quelli di *privacy by default* e di *privacy by design* (art. 25 GDPR) rendono la normativa di protezione dei dati personali una disciplina non solo da attuare, ma, più propriamente, da tradurre in soluzioni pratico/operative determinate dalla *expertise* o dall'inventiva degli operatori. La regolazione delle autorità, infatti, realizza una naturale funzione di verifica di secondo livello della correttezza delle soluzioni organizzative e tecnologiche adottate dagli utilizzatori delle informazioni. Per questo, diventa una regolazione relativa al controllo delle scelte e delle soluzioni tecniche[5] e si espande, fisiologicamente, in ogni ambito delle attività realizzate con apparati tecnologici, meccanizzati o digitali (ad esempio, fino a regolare l'inclinazione ed il *focus* delle apparecchiature di videosorveglianza o la tipologia di informazioni registrate da apparecchi di geolocalizzazione che gestiscono la manutenzione di autoveicoli concessi in locazione).

Spinge nella direzione dell'estensione della regolazione di *data protection* anche la progressiva importanza assunta dalla base giuridica del legittimo interesse (GDPR art. 6, comma 1, lett. f) a discapito delle altre basi di derivazione civilistica – cioè radicate nel valore dell'equilibrio tra posizioni correlate in un rapporto diretto a realizzare contrapposti interessi – quali il consenso e la necessità di eseguire un contratto richiesto dall'interessato (GDPR art. 6, comma 1, lett. a e b)[6]. Infatti, considerata l'indeterminatezza della figura[7], che oscilla tra interessi non espressamente vietati ed interessi meritevoli di tutela per la loro funzionalità socio/economica, le autorità indipendenti si sentono in dovere di imporre fitte "reti di contenimento" normativo ai trattamenti fondati su questo presupposto di liceità[8]. Ed anche questo concorre a dilatare l'ambito di operatività della regolazione amministrativa.

Infine, l'impianto normativo del GDPR, pur con alcune differenziazioni, contempla un sistema disciplinare comune per il trattamento dei dati personali diretto a realizzare interessi privati e per quello diretto a realizzare, anche oggettivamente, interessi pubblici (come risulta dal combinato disposto degli artt. 6 e 55 del Regolamento)[9]. Anche così si rende espansiva la regolazione.

Considerate le ragioni dell'espansione dell'azione delle autorità amministrative di *data protection* è necessario considerare come essa si stia realizzando concretamente. A questo proposito, sembra che questa tendenza si produca in due modi diversi: attraverso un "recesso sostanziale" di altre discipline, che, per cosi dire, riducono il proprio ambito di applicazione in via interpretativa, in esito all'azione della giurisprudenza e della stessa regolazione; attraverso un "recesso formale" di altre discipline che riducono il proprio ambito di applicazione in via normativa, per effetto di specifiche disposizioni del legislatore.

Denominatore comune di queste due modalità, peraltro, è che l'espansione avviene, oltre che per i fattori già considerati, perché la *data protection* viene sostanzialmente percepita come uno strumento più adeguato ed efficace per garantire i diritti fondamentali. In altri termini, è un criterio interpretativo e normativo di prevalenza a dettare l'espansione della regolazione.

2. I casi recenti di applicazione espansiva della *data protection* in differenti ambiti normativi

È possibile tracciare una panoramica di esempi delle forme di recesso di cui sopra.

4. Sul quale Galli 2023.
5. Su questi temi Yeung–Bygrave 2022, spec. p. 141.
6. Cfr. su questa base giuridica le recenti indicazioni generali di European Data Protection Board, *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR*, Versione 1.0, 8 ottobre 2024.
7. Recentemente, Bonomi Madec–Vasileiadou 2025.
8. Sottolinea come questa azione regolatoria si traduca in una sistematica imposizione dell'interesse pubblico alla correttezza di trattamento Proietti 2022.
9. Il tema del trattamento pubblico dei dati è stato recentemente illustrato da Franca 2023.

Con la nota sentenza C-252 del 2023 (*Meta Platform*) la Corte di giustizia Ue[10] dà corso al recesso della normativa a tutela della concorrenza a vantaggio di quella di *data protection*. I Giudici, nel valutare l'irrogazione di una sanzione antitrust dell'autorità tedesca, affermano che l'"incrocio" di dati personali (cioè la trasmissione delle preferenze dei clienti ad investitori pubblicitari) da parte di un social network è illecito con riguardo alla disciplina del loro trattamento. Infatti, esso non trova fondamento giuridico né nel consenso dell'interessato, né nella necessità di eseguire il contratto di utilizzo della rete sociale, né in un legittimo interesse del titolare.

L'elemento rilevante della sentenza, però, è che la violazione delle regole del GDPR rappresenta l'elemento costitutivo della fattispecie di abuso di posizione dominante di cui all'art. 102 del TFUE. In altri termini, un trattamento illecito di dati personali può rappresentare lo strumento per alterare le dinamiche della concorrenza. Per questo, secondo la Corte, le autorità antitrust nazionali, prima di irrogare una sanzione per un comportamento anticoncorrenziale, determinato da una pretesa violazione del diritto alla protezione dei dati personali, debbono fare riferimento ai precedenti provvedimenti sanzionatori delle autorità di *data protection*, per considerare se il comportamento di cui è causa sia stato precedentemente qualificato come illecito. Conseguentemente debbono attenersi alla "giurisprudenza" o prassi regolatoria delle autorità. Nel caso, poi, in cui non vi siano precedenti regolatori in termini, la sentenza impone alle autorità antitrust di coinvolgere nel procedimento i Garanti per la protezione dei dati personali, fornendo loro un termine entro il quale qualificare i comportamenti in esame. Solo spirato questo termine, le amministrazioni procedenti antitrust potranno assumere le loro determinazioni sanzionatorie[11].

Come si vede, la Corte impone un recesso della regolazione (e della normativa) antitrust a vantaggio di quella di *data protection*, chiamata ad identificare i trattamenti scorretti di informazioni personali sostanzialmente in grado di alterare illecitamente anche le dinamiche di mercato. È interessante considerare, poi, come, in questo caso di recesso, la normativa sul trattamento dei dati personali vada oltre la propria *mission* originaria di protezione dei diritti fondamentali, per ridondare nella garanzia degli interessi del mercato.

Un altro interessante esempio di recesso formale è rappresentato dalla sentenza del Consiglio di Stato n. 497 del 2024 che ripropone lo stesso itinerario argomentativo della Corte di giustizia, collocandolo, però, nella materia della tutela del consumatore. In questo caso, i giudici valutano l'applicazione di sanzioni irrogate dall'autorità antitrust a tutela dei consumatori ed affermano che una società commerciale che fornisce ai propri clienti informazioni ingannevoli sull'utilizzo dei loro dati personali (trasmessi senza consenso ad inserzionisti commerciali che li utilizzano per concludere nuovi contratti) li utilizza in maniera scorretta ai sensi del Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196, art. 130). Ma questo comportamento rappresenta anche l'elemento costitutivo della violazione dei diritti dei consumatori attribuiti dall'art. 67-*sexdecies* del Codice del consumo (d.lgs. 6 settembre 2005, n. 206) che li protegge dalle comunicazioni commerciali non richieste[12].

10. Corte giustizia Ue, Grande Sezione, sent. 4 luglio 2023, n. 252, in "Foro it."2023, 12, IV, 580.

11. Sulle dinamiche di coordinamento delle autorità cfr. per tutti Manzini 2023; Parona 2024.

12. La sentenza segue nella sostanza la precedente giurisprudenza dello stesso Consiglio di Stato (Consiglio di Stato, Sez. VI, 29 marzo 2021, n. 2630, in "Dejure" e Consiglio di Stato, Sez. VI, 29 marzo 2021, n. 2631 in "Foro it.", 2021, 6, III, 325) che aveva affermato, con una ricostruzione normativa differente, perché non ancora condizionata dalla giurisprudenza della Corte di giustizia Ue, che una violazione degli obblighi di informazione del GDPR avrebbe potuto rilevare non in sé stessa, ma come violazione degli obblighi a tutela dei consumatori, che avrebbe rappresentato l'unico illecito giuridicamente rilevante. Le sentenze avevano la singolare intenzione di limitare l'applicazione diretta della *data protection* in ambito economico evitando che il GDPR erodesse l'applicazione delle altre discipline astrattamente applicabili ed estendesse "il proprio ambito di applicazione fin dove può giungere qualsiasi forma di relazione umana o automatica del dato personale", p. 23 sent. 2631. Per questo, i giudici avevano limitato la *data protection* affermando che essa protegge solo i diritti personalissimi e non quelli di segno economico, rimessi alla tutela di altre normative. Il tentativo, peraltro, non aveva condotto a

I giudici, correlativamente, affermano il necessario coinvolgimento, nella procedura di irrogazione di sanzioni a tutela del consumatore, del Garante per la protezione dei dati personali, proprio perché l'illecito consumeristico è realizzato violando la normativa di *data protection*, le cui modalità di applicazione non possono che essere determinate dalla relativa amministrazione di regolazione.

Anche in questo caso, come nella giurisprudenza della Corte di giustizia, la normativa e la regolazione di tutela del consumatore recedono a vantaggio della normativa e della regolazione a tutela dei dati personali. Qui, però, siamo di fronte a discipline e funzioni amministrative che hanno tutte lo stesso obiettivo di proteggere i diritti fondamentali di segno economico delle persone. La protezione dei dati personali, però, viene fatta prevalere, perché è percepita come più efficace. Infatti, i giudici le lasciano l'ultima parola sulle modalità di garanzia delle ragioni del consumatore.

Un altro esempio di recesso sostanziale è rappresentato dalla giurisprudenza italiana recente in materia di controlli difensivi in senso stretto (ovvero quei controlli realizzati *ex post* dal datore di lavoro nei confronti di lavoratori con riguardo ai quali sia sorto il sospetto che abbiano violato i propri doveri o abbiano pregiudicato gli interessi dell'azienda) ed in particolare dalla sentenza della Corte di Appello di Venezia di data 22 maggio 2024[13].

Questi controlli sono tradizionalmente sottratti dalla giurisprudenza dall'ambito di applicazione dell'art. 4 dello Statuto dei lavoratori (legge 40 maggio 1970, n. 300), che li sottopone al rispetto dei principi del Codice in materia di protezione dei dati personali. Nonostante ciò, la sentenza afferma che questo tipo di verifiche, nella fattispecie indagini e investigazioni private, debbono sottostare alla *data protection*. Questo perché, sulla scorta degli insegnamenti della giurisprudenza CEDU[14], incidono sulla dignità del lavoratore e, per essere sostenibili, con riferimento ai diritti fondamentali, debbono osservare i principi di necessità, proporzionalità, legittimità delle finalità, ecc… della normativa che protegge i dati personali. E questi principi sono attuati, qui, dalla regolazione del Garante nazionale[15]. Sulla base di queste considerazioni, quindi, i giudici nazionali affermano che le investigazioni difensive dirette a verificare l'autenticità dello stato di malattia, ulteriori rispetto agli accertamenti delle autorità pubbliche, sono incongrue se contrarie alle linee guida in materia poste dall'Autorità di protezione dei dati personali. E questo rende illecito il conseguente licenziamento.

Anche in questo caso, nella sostanza, l'illecito di *data protection* integra l'elemento costitutivo di un illecito lavoristico ed è possibile ipotizzare che, nel prossimo futuro, la giurisprudenza italiana, proprio come hanno fatto i giudici europei, affermi in maniera esplicita e formale questa dinamica.

Occorre considerare che, in questo caso, la protezione dei dati ed il diritto del lavoro condividono l'obiettivo di proteggere i diritti fondamentali. Tuttavia, il prevalere della prima normativa – che impone determinate modalità di trattamento dei dati, considerate maggiormente "sostenibili" con riferimento alla protezione della dignità personale – supera la logica lavoristica, modellata sulla ricerca dell'equilibrio di posizioni corrispettive

limitare nel concreto la normativa di protezione dei dati personali che era riuscita a condizionare nella sostanza se non nella forma i canoni di applicazione della disciplina di tutela del consumatore. Sulle sentenze Franca 2021; sia consentito rinviare anche a Midiri 2021.

13. In "Il lavoro nella giurisprudenza", 2024, p. 1135 con nota di M. D'Aponte 2024 che cita come precedenti in termini Cass. n. 17723/2017; Cass. n. 25732/2021; Cass. n. 18168/2023.

14. SI fa riferimento alla nota sentenza della Corte Europea dei Diritti dell'Uomo del 5 settembre 2017 – Ricorso n. 61496/08 – *Barbulescu c. Romania*.

15. A questo proposito la sentenza cita le "Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria" (Provvedimento del Garante per la protezione dei dati personali n. 60/2008) poi trasposte nelle Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 – 19 dicembre 2018 (Pubblicato sulla Gazzetta Ufficiale n. 12 del 15 gennaio 2019) Registro dei provvedimenti n. 512 del 19 dicembre 2018.

collegate in un rapporto bilaterale datore di lavoro/lavoratore. In altri termini, si impongono modalità di svolgimento di attività private (oggetto di regolazione amministrativa pubblica) piuttosto che regole di equilibrio di una relazione giuridica.

Nella dimensione del diritto del lavoro, peraltro, è possibile rilevare anche dinamiche di recesso "formale" oltre che sostanziale. Infatti, lo stesso art. 4 dello Statuto dei lavoratori, che, come abbiamo visto, fa riferimento ai controlli difensivi in senso ampio (cioè quei controlli sistematici per la difesa soprattutto dei beni aziendali) impone, nella loro realizzazione, l'applicazione dei principi di protezione dei dati personali. In questo caso, è lo stesso legislatore a disporre che la normativa di protezione dei dati personali condizioni gli esiti applicativi del diritto del lavoro e del diritto sindacale. Correlativamente, il Garante ha sviluppato un'intensa attività di regolazione che disciplina lo svolgimento di attività come la videosorveglianza, il controllo della posta elettronica aziendale, l'analisi dei metadati dei computer aziendali[16]. In sostanza, l'amministrazione pone le coordinate normative all'interno delle quali, ferma l'applicazione delle regole di diritto del lavoro e delle dinamiche sindacali, debbono svolgersi i poteri di controllo, disciplinari e sanzionatori del datore di lavoro. Anche in questo modo, le violazioni della *data protection* finiscono per rappresentare, sostanzialmente, l'elemento costitutivo di illeciti giuslavoristici.

Esistono, ancora, casi di recesso sostanziale in grado di produrre i propri effetti nella dimensione dell'attività amministrativa e del provvedimento.

La Corte di giustizia Ue ha pronunciato alcune recenti sentenze nelle quali si è interrogata sulla legittimità giuridica generale di decisioni di *credit scoring* (cioè della attribuzione interamente automatizzata a un cliente di un servizio finanziario di un punteggio che determina la sua solvibilità e, quindi, il possibile accesso a rapporti contrattuali di varia natura). Con la sentenza C-634/2023 (*Schufa*)[17] la Corte risolve il problema utilizzando un parametro normativo tratto dalla *data protection*, ovvero l'art. 22 del GDPR (rubricato "Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione").

I Giudici, a questo riguardo, affermano che il *credit scoring* è qualificabile come una decisione interamente automatizzata, perché incide sulla sfera giuridico-soggettiva del destinatario. Nello stesso tempo affermano che essa è lecita, in senso generale, se fondata sui presupposti di legittimità di trattamento dello stesso art. 22: la presenza di una norma di diritto europeo o nazionale – anche di una disposizione che disciplini attività di interesse pubblico – che l'autorizzi, garantendo il rispetto dei diritti fondamentali; la messa a disposizione di procedure di reclamo con intervento umano che assicurino la correttezza di merito della decisione; il rispetto di tutti i principi normativi generali della protezione dei dati personali (ovvero tutti quelli indicati negli artt. 5, 6 e 25 del GDPR).

Viene affermato con decisione, quindi, che un atto interamente automatizzato, anche adottato in assenza di un intervento umano, è pienamente lecito se è previsto dalla legge, ma, soprattutto, se segue tutti i parametri di trattamento delle informazioni personali, parametri che ne rappresentano il vero metro di ammissibilità.

La sentenza supera la *vulgata* pubblicistica, consolidatasi recentemente, secondo la quale un provvedimento amministrativo privo dell'intervento umano nella sua fase di formazione sarebbe illegittimo[18], a più forte ragione se di carattere discrezionale[19]. Impone, invece, come nuovi parametri di liceità, prima che di legittimità, i principi della *data protection*.

In questa nuova ricostruzione, allora, principi come la funzionalizzazione del trattamento dei dati (alla base della decisione automatizzata) per le finalità legittime previste dalla legge, la correttezza del trattamento stesso e la veridicità dei dati finiranno per rappresentare, nella dimensione provvedimentale, una versione aggiornata di categorie

16. Fragassi 2024. Ma in generale su tutti i temi relativi ai controlli difensivi cfr. la panoramica di Rotondi–Tursi 2025.
17. Corte giustizia Ue, sez. I, 7 dicembre 2023, causa C-634/21, in "Nuova giurisprudenza civile commentata", 2024, 416, con nota di D'Orazio 2024, sulla sentenza anche Pietrella–Racioppi 2024.
18. Per tutti Stacca 2024; Grenci 2024.
19. In questi casi, come afferma la giurisprudenza, la discrezionalità verrebbe riallocata "a monte" nella definizione dell'algoritmo, su questi temi Botto 2024 e bibliografia ivi citata.

come l'eccesso di potere per sviamento, la contraddittorietà tra atti del procedimento, l'incompletezza dell'istruttoria o il travisamento dei fatti. Certamente, si tratta di nuovi parametri che non sostituiranno i vecchi, primo fra tutti il canone della trasparenza, su cui tanto ha insistito a ragione la dottrina[20], ma si affiancheranno ad essi, per fondare un nuovo sindacato di legittimità del provvedimento algoritmico. Ed è inutile dire che tutti questi parametri, in futuro, saranno definiti, nel concreto, dalla regolazione amministrativa.

Tutti questi parametri saranno utili per contestare decisioni algoritmiche sbagliate, anche senza passare dalla piena conoscenza dei modelli che hanno guidato i sistemi (modelli che nella IA sono irrecuperabili agli stessi programmatori per i noti fenomeni di *black box*). Proprio come ha sostanzialmente fatto una recente sentenza della Corte di giustizia che ha ipotizzato l'irragionevolezza di una decisione di *credit scoring* che non ammetteva una persona ad un contratto telefonico con canone di soli dieci euro al mese per i suoi trascorsi di cattivo pagatore[21]. Ma in quest'ottica appariranno implausibili anche gli algoritmi di assegnazione degli incarichi di insegnamento ai supplenti precari che attribuiscono incarichi didattici a persone con punteggio inferiore e li negano ad altre con punteggio superiore, violando il principio di verità dei dati personali prima di quello di efficacia della funzione di istruzione[22].

Per concludere sul punto, anche nel caso del *credit scoring*, la normativa di protezione dei dati personali si impone come parametro di liceità giuridica generale per la sua maggiore capacità di proteggere i diritti della persona con riguardo allo svolgimento di ogni attività automatizzata, pubblica o privata, ammessa dalla legge.

Sono stati indicati i casi più recenti e rilevanti di recesso sostanziale e formale, ma occorre considerare che non si tratta degli unici. In vari altri campi, infatti, è la stessa regolazione ad imporre, all'interno di sistemi normativi specifici, norme *ad hoc*, che rappresentano lo sviluppo o l'adattamento di regole generali di *data protection*. Ad esempio, l'EDPB ha recentemente imposto alcune prescrizioni specifiche per l'utilizzo di modelli di intelligenza artificiale[23], indipendentemente dall'applicazione del recente regolamento europeo in materia[24]. Ancora, il Garante italiano ha emanato un vademecum sulla privacy a scuola che introduce regole in grado di incidere sulle modalità di svolgimento dell'attività didattica (come la definizione di tracce di temi o la loro lettura in classe, le modalità di svolgimento della videolezione, il controllo dei docenti sull'utilizzo di social network per prevenire fenomeni di cyberbullismo o simili)[25].

3. Alcune considerazioni sull'ammissibilità di questa vocazione espansiva della normativa e della regolazione di *data protection*

Esaurita questa panoramica è possibile considerare come, per il tramite della regolazione, si stia realizzando un'estensione sostanziale dell'ambito di

20. Carloni 2024.
21. Corte giustizia Ue, sez. I, sent. 27 febbraio 2025, causa C-203/22, pur anche in questo caso affermando l'obbligo di trasparenza anche in presenza di segreti industriali.
22. Cfr. Tribunale di Roma, sent. n. 1463/2023 pubbl. il 10 febbraio 2023 sulla quale Rivellini 2023, ma ancora più chiara, tra le altre di medesimo tenore, Tribunale di Torino, sent. n. 1232/2025 del 15 maggio 2025. In estrema sintesi, l'algoritmo ministeriale consentiva ai docenti, prima dell'inizio dell'anno scolastico, di identificare una serie di scuole di loro preferenza. Una volta effettuato il primo giro di chiamate senza che si fossero rese disponibili scuole di loro gradimento il sistema considerava questi stessi docenti rinunciatari su tutte le scuole (anche quelle scelte) per tutte le eventuali tornate successive (forse per ragioni legate ad una più agevole programmazione degli algoritmi). Resisi disponibili successivamente incarichi nelle scuole di preferenza i docenti venivano logicamente pretermessi ed il sistema procedeva alla chiamata di altri docenti, naturalmente collocati più in fondo nelle liste e con minore punteggio.
23. Cfr. European Data Protection Board, *Opinion n. 8/2024 on certain data protection aspects related to the processing of personal data in the context of AI models* (adottata il 17 dicembre 2024).
24. Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024.
25. Cfr. Garante per la protezione dei dati personali *Vademecum La scuola a prova di privacy*, 2023.

applicazione della disciplina della *data protection*. Essa tende oggi ad identificarsi con l'ambito della protezione dei diritti fondamentali e, più, in generale, della dignità della persona nei confronti delle attività umane realizzate con strumenti tecnologici, cioè di tutte[26]. In sostanza, si scrive protezione dei dati personali ma si legge garanzia dei diritti inviolabili dell'uomo, secondo il riferimento classico del nostro art. 2 della Costituzione. Si tratta di una tendenza ormai irreversibile di politica del diritto a cui è necessario adattarsi.

Peraltro, da un punto di vista giuridico, non è necessario fare considerazioni di ordine politico o sociale e chiedersi se si tratta di una tendenza efficace o utile. È necessario, invece, chiedersi se si tratti di una tendenza ammissibile nell'ambito delle coordinate giuridico istituzionali europee e nazionali. Non si deve dimenticare, infatti, che spesso queste forme di recesso conducono all'applicazione di norme derivate dalla protezione dei dati personali in ambiti nei quali il legislatore non le ha volute o all'irrogazione di conseguenti sanzioni per infrazioni non direttamente previste in differenti settori disciplinari.

La soluzione sembra potere essere quella, classica ma sempre attuale[27], di applicare un rigido principio di legalità riferito alle norme attributive ed alle condizioni di validità del potere di regolazione, che è il vero strumento di questa estensione sostanziale. Non si tratta, come si vede, di utilizzare il principio di legalità come parametro di legittimità per le attività di trattamento pubbliche e private, come ha ben fatto la dottrina recente[28], ma di applicarlo per condizionare le differenti funzioni delle amministrazioni di regolazione, che controllano, sanzionano e disciplinano quelle attività.

Applicare il principio di legalità alle funzioni di regolazione delle amministrazioni indipendenti nazionali ed europee significa imporre, come obiettivi e come coordinate fondamentali delle loro competenze, i due interessi pubblici che il legislatore europeo ha posto a fondamento del GDPR: la tutela dei diritti fondamentali e la libera circolazione dei dati personali (art. 1 ed art. 55 per le Autorità). I Garanti del trattamento dei dati debbono esercitare le loro funzioni tenendo conto che si tratta dei due pilastri fondamentali della *data protection* e che, nell'attuazione della normativa (vera *mission* delle Autorità ex art. 55 del GDPR), debbono essere realizzati insieme e debbono rimanere integrati e coordinati. In caso contrario, si scivolerà verso una disciplina squilibrata, esclusivamente difensiva, formalistica ed in grado di condizionare oltremisura anche tutti i campi di attività dove la protezione dei dati personali viene "esportata".

Tutto ciò può essere realizzato esercitando le funzioni di regolazione secondo un rigido principio di "lesività" delle attività di trattamento. In altri termini, le amministrazioni indipendenti, nella loro normazione di carattere tecnico, nella qualificazione degli illeciti e nell'applicazione delle sanzioni, dovranno identificare, come comportamenti sostanzialmente contrari alle regole dell'ordinamento, quelli in grado, non soltanto di violare forme, procedure, obblighi o principi del GDPR, ma quelli in grado di recare pregiudizio reale ai diritti inviolabili garantiti attraverso il diritto alla protezione dei dati personali. In caso contrario, la protezione dei dati perderà il suo equilibrio, ma anche la sua ragione d'essere, che è quella di rendere lo sviluppo tecnologico sostenibile e compatibile con la dignità umana.

Del resto, la stessa giurisprudenza in materia di risarcimento del danno da trattamento illecito dei dati, pur relativa ad altra materia, afferma il principio secondo il quale una violazione delle disposizioni del GDPR non è di per sé sufficiente a costituire un "danno risarcibile"[29].

26. Cfr. a questo proposito Simoncini 2023, che afferma che la tecnologia è ormai trasversale e necessaria per ogni aspetto della vita umana. È utile e veloce ma con un incomparabile impatto sui diritti. Diventa un potere privato che serve ad informare ed a sostituire la decisione umana, ovvero un potere nei confronti del quale si registra la inadeguatezza della normazione parlamentare classica a vantaggio della self regulation e coregulation.
27. Si tratta di un principio che giovani studiosi hanno utilmente utilizzato per risolvere questioni anche più complesse cfr. per tutti Vaccari 2024; Vettori 2024.
28. Ponti 2023.
29. Corte giustizia Ue, sez. VIII, 4 ottobre 2024, causa C-507/23; Corte giustizia Ue, sez. III, 20 giugno 2024, causa C-590/22; Corte giustizia Ue, sez. III, 11 aprile 2024, causa C-741/21.

Riferimenti bibliografici

S. Bonomi Madec, G. Vasileiadou (2025), *Understanding Legitimate Interest under the GDPR: A study of the CJEU Case C-621/22 and the EDPB Guidelines*, in "Global Privacy Law Review", vol. 6, 2025

G. Botto (2024), *Decisone algoritmica, discrezionalità e sindacato del giudice amministrativo*, in "Federalismi.it", vol. 17, 2024

E. Carloni (2024), *Transparency within the artificial administration, principles, paths, perspectives and problems*, in "Italian Journal of Public Law", vol. 16, 2024

M. D'Aponte (2024), *I controlli difensivi devono soggiacere ai principi di giustificatezza, proporzionalità e minimizzazione dei dati trattati*, in "Il Lavoro nella Giurisprudenza", vol. 12, 2024

F. D'Orazio (2024), *Il credit scoring e l'art. 22 del GDPR al vaglio della Corte di giustizia*, in "Nuova Giurisprudenza Civile Commentata", vol. 2, 2024

A. Fragassi (2024), *L'instabile equilibrio tra controllori e controllati nello sguardo del Garante privacy*, in "Labour & Law Issues", vol. 10, 2024

S. Franca (2023), *I dati personali nell'amministrazione pubblica. Attività di trattamento e tutela del privato*, Editoriale Scientifica, 2023

S. Franca (2021), *L'intreccio fra disciplina delle pratiche commerciali scorrette e normativa in tema di protezione dei dati personali: il caso Facebook approda al Consiglio di Stato*, in "Rivista della Regolazione dei Mercati", vol. 2, 2021

F. Galli (2023), *Il principio di accountability*, in L. Califano, V. Fiorillo, F. Galli (a cura di), "La protezione dei dati personali: natura, garanzie e bilanciamento di un diritto fondamentale", Giappichelli, 2023

S.B. Grenci (2024), *Le applicazioni di Intelligenza artificiale a supporto dell'automazione del procedimento amministrativo*, in "Rivista Italiana di Informatica e Diritto", 2024, n. 1

P. Manzini (2023), *Antitrust e privacy: la strana coppia*, in Id. (a cura di), "I confini dell'antitrust – Diseguaglianze sociali, diritti individuali, concorrenza", Giappichelli, 2023

F. Midiri (2021), *Proteggere i dati personali con le tutele del consumatore*, in "Giornale di Diritto Amministrativo", vol. 5, 2021

F. Midiri (2019-a), *Commento all'art. 51, Regolamento UE 27 aprile 2016, n. 2016/679 in materia di protezione dei dati personali (c.d. GDPR)*, in A. Barba, S. Pagliantini (a cura di), "Commentario del Codice Civile", Utet, 2019

F. Midiri (2019-b), *Commento all'art. 57, Regolamento UE 27 aprile 2016, n. 2016/679 in materia di protezione dei dati personali (c.d. GDPR)*, in A. Barba, S. Pagliantini (a cura di), "Commentario del Codice Civile", Utet, 2019

F. Midiri (2019-c), *Commento all'art. 58, Regolamento UE 27 aprile 2016, n. 2016/679 in materia di protezione dei dati personali (c.d. GDPR)*, in A. Barba, S. Pagliantini (a cura di), "Commentario del Codice Civile", Utet, 2019

F. Midiri (2017), *Il diritto alla protezione dei dati personali*, Editoriale Scientifica, 2017

L. Parona (2024), *Addressing the interplay between competition law and data protection law in the digital economy through administrative cooperation: the CJEU judgment in the Meta Platforms case*, in "Italian Journal of Public Law", vol. 16, 2024

V. Pietrella, S. Racioppi (2024), *Il credit scoring e la protezione dei dati personali: commento alle sentenze della Corte di giustizia dell'Unione europea del 7 dicembre 2023*, in "Rivista Italiana di Informatica e Diritto", 2024, n. 1

B. Ponti (2023), *Attività amministrativa e trattamento dei dati personali. Gli standard di legalità tra tutela e funzionalità*, FrancoAngeli, 2023

G. Proietti (2022), *Algoritmi e interesse del titolare del trattamento nella circolazione dei dati personali*, in "Contratto e Impresa", vol. 3, 2022

G. Rivellini (2023), *L'errore dell'algoritmo obbliga la pubblica amministrazione a risarcire il danno*, in "www.irpa.eu – Osservatorio sullo Stato digitale", 14 giugno 2023

F. Rotondi, A. Tursi (2025), *I controlli sull'attività dei lavoratori alla prova dell'intelligenza artificiale*, in "Il Lavoro nella giurisprudenza", vol. 2, 2025

A. Simoncini (2023), *Sistema delle fonti e nuove tecnologie. Le ragioni di una ricerca di diritto costituzionale, tra forma di Stato e forma di governo*, in Id. (a cura di), "Sistema delle fonti e nuove tecnologie. Il ruolo delle autorità indipendenti", Giappichelli, 2023

S. Stacca (2024), *Potere algoritmico. Profili organizzativi del rapporto tra amministrazione e automazione*, in "Diritto Pubblico", vol. 2, 2024

S. Vaccari (2024), *L'invalidità parziale del provvedimento amministrativo*, Giappichelli, 2024

N. Vettori (2024), *Autorità indipendenti e concentrazione dei poteri: distinzione delle funzioni a garanzia dei diritti*, Editoriale Scientifica, 2024

K. Yeung, L.A. Bygrave (2022), *Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship*, in "Regulation & Governance", vol. 16, 2022

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0243 • articolo sottoposto a peer review • pubblicato in anteprima il 4 dic. 2025

Fabio Bravo

L'intermediazione dei dati e la sua evoluzione dal settore privato a quello pubblico

Il presente contributo si propone di analizzare gli aspetti giuridici dell'intermediazione dei dati, quale fenomeno che, sorto ed affermatosi nel settore privato, ha avuto un'espansione considerevole anche nel settore pubblico, grazie anche all'evoluzione normativa dell'ordinamento europeo, non slegata dalle dinamiche di regolazione del mercato. Il contributo, prendendo criticamente in esame le relazioni sussistenti tra intermediazione di dati, diritto alla portabilità e delega, anche alla luce dei provvedimenti resi dalle Authority di settore, conduce la disamina sull'intermediazione di dati nel recente quadro normativo delineato dal legislatore europeo in materia di Spazi europei di condivisione di dati sanitari, indagando i margini di applicazione degli istituti in esame di fronte a tale specifico settore.

Intermediazione di dati – Dati personali e governance dei dati – Diritto alla portabilità dei dati – Delega

Data intermediation and its evolution from the private to the public sector

This contribution examines the legal aspects of data intermediation, a phenomenon that originated in the private sector and has since extended into the public sector, in part owing to developments in European Union legislation and market-regulation dynamics. The author critically analyses the interaction between data intermediation, the right to *data portability* and delegation, with particular reference to decisions issued by sectoral authorities. It considers data intermediation in the context of the recent regulatory framework enacted by the European legislator for European Health Data Spaces, and assesses the applicability of the relevant legal constructs within that domain.

Data intermediation – Personal data and data governance – Data portability – Delegation

L'Autore è professore ordinario di Diritto privato, Alma Mater Studiorum Università di Bologna

Questo contributo fa parte della sezione monografica *I dati in ambito pubblico tra esercizio della funzione amministrativa e regolazione del mercato*, a cura di Marco Bombardelli, Simone Franca, Anna Simonati

1. Obiettivi e direzione del discorso

Il fenomeno dell'intermediazione dei dati, sviluppatosi soprattutto in ambito privato, sta acquisendo nuove prospettive con l'evoluzione dell'ordinamento europeo, delle tecnologie e dei modelli di *business* che si vanno consolidando nel mercato. Si tratta però di fenomeno a cui il settore pubblico non è estraneo ed ha ora assunto margini di espansione notevoli, la cui regolamentazione finisce per impattare inevitabilmente sul mercato, traducendosi, direttamente o indirettamente, anche in uno strumento di regolazione di mercato[1].

Il presente contributo si colloca proprio in tale direzione, avendo come obiettivo quello di indagare l'intersezione tra il fenomeno di "data intermediation", di origine privatistica, i "dati in ambito pubblico" e le criticità che si riverberano sulla "regolazione del mercato", di fronte agli sviluppi normativi unionali.

Il discorso trova il suo culmine proprio nella nuova disciplina sugli spazi di condivisione dei dati sanitari, in cui l'intermediazione guadagna nuovi campi di intervento, ma subisce anche nuove ed incisive spinte regolatorie suscettibili di impattare pesantemente sul mercato. Sicché proprio il recente Regolamento EHDS costituisce, in tale prospettiva, il banco di prova per testare la relazione tra i tre predetti elementi dell'indagine – *data intermediation, data in public sector e market regulation* – e per individuare, in chiave evolutiva, sia le criticità emergenti, sia i possibili percorsi per il loro superamento.

1. In materia si veda, per un inquadramento, Bombardelli 2023.

2. L'intermediazione dei dati. Genesi e sviluppo

2.1. Il caso americano: Lumeria

Le radici dell'intermediazione dei dati possono essere rinvenute verso la fine degli anni Novanta del secolo scorso[2], allorché venne posta attenzione, nella letteratura di settore, all'emergente ruolo delle *data company* che – quali nuovi *infomediaries* – svolgevano compiti di intermediazione in favore degli interessati, ponendosi quali nuove figure sul mercato in grado di agire per loro conto, negoziando in loro favore le migliori condizioni per l'utilizzo e la remuneratività dei dati medesimi e offrendo loro, al contempo, adeguati strumenti di controllo su tali dati, prima di riversarli sul mercato[3].

Si stavano affacciando nuovi imprenditori, capaci di intercettare nuovi modelli di *business* nell'emergente e inesplorato terreno dei *data markets*. Tra questi, uno dei pionieri è sicuramente Lumeria, società californiana operante già dalla fine del Novecento nel settore commerciale dell'*identity management* e della "*consumer privacy*": nell'ambito dei propri servizi aveva iniziato a fornire alle persone fisiche (*data subjects*) specifici strumenti per proteggere, condividere con altri (in termini di utilizzo commerciale) e dunque valorizzare i loro dati personali, ponendosi come soggetto capace di agire in nome e per conto dei medesimi, per la cura dei loro interessi[4]. Si poneva dunque quale loro rappresentante e mandatario, proteggendo ed estraendo valore dai loro dati personali, che venivano memorizzati in appositi database gestiti da tale società[5].

Le modalità operative di tale modello di *business*, estremamente significativa ai fini del nostro discorso, si colgono molto bene nelle parole del fondatore e amministratore delegato della predetta società, nella parte in cui ha precisato che "Our model was that the individual should be able to control what information is shared with what entities – people, Web sites, commerce partners, whatever. What we needed was a system that could present information about you without revealing who you are, not even to us at Lumeria. So what I did was, I went out and hired a bunch of hackers and security nuts, and said, 'Let's re-engineer. Let's create a system that is comprehensive enough so that even when all of your information – browsing habits, medical data, bank accounts, school transcripts – becomes digitized and moves into the Internet age, you can have a unified way to control and reveal and protect it.' Basically, we created a new piece of Internet infrastructure for the secure communication and authentication of transmissions across the Internet. It took us a few years and millions of dollars to develop it, but now it's here, and it's pretty cool. The consumer has complete control for the first time. And the legislative future plays into our hands. Soon we'll be a compliance mechanism for new privacy regulations. It's a great sell. It's a no-brainer. *Businesses* won't have to understand all of the great things we do for our customers. It's just, the feds are going to bust you if you don't use it!"[6].

Altrettanto significative sono le ulteriori parole spese per descrivere i meccanismi di funzionamento sia dell'intermediazione dei dati, sia le modalità

2. Cfr. Bravo 2020 e Bravo 2021.
3. In questo senso si veda Hagel–Rayport 1997-a, i quali, con una lucida analisi di mercato, anticipando i tempi, ebbero modo di evidenziare che "Companies have good reason to collect information about customers. It enables them to target their most valuable prospects more effectively, tailor their offerings to individual needs, improve customer satisfaction and retention, and identify opportunities for new products or services. But even as more and more managers begin to build strategies based on capturing information about their customers, a major change is under way that may undermine their efforts. We believe that consumers are going to take ownership of information about themselves and demand value in exchange for it. As a result, negotiating with consumers for information will become costly and complex. That process has already begun to unfold, but it could take several years to play out across broad segments of customers and products". Nello stesso senso v. anche Hagel–Rayport 1997-b, p. 54 ss.
4. Cfr. Lester 2001.
5. *Ibidem*.
6. *Ibidem*.

per ottenere redditività tanto per la società di intermediazione, quanto per gli interessati loro clienti: "A customer will store personal data in what is called a SuperProfile. The more specific the information stored (about such things as age, sex, family status, sexual orientation, income level, assets, consumer preferences, and current shopping interests), the more valuable that profile will become to advertisers, who will pay handsomely to participate in Lumeria's network. They will do this because Lumeria will give them the chance to do highly targeted, permission-based marketing – to offer special deals on, say, new cars or house-painting services or plane tickets – exclusively to people of a predetermined demographic profile, and often only to people who have already expressed an interest in the very things being advertised. Most of the money from advertisers will go directly to Lumeria's users; Lumeria will take a small cut"[7].

2.2. L'importazione del modello americano in Italia: il caso Hoda (Weople). L'impatto dell'intermediazione dei dati e della *data portability* sulle dinamiche concorrenziali nei *data markets*

Tale modello, in Italia, è stato importato da Hoda, società milanese attiva nell'intermediazione di dati, che ha ben interpretato nel contesto europeo le dinamiche di mercato americane, calandole efficacemente entro i margini di operatività della disciplina sulla protezione dei dati personali, grazie anche all'innovazione avutasi con l'introduzione del diritto alla portabilità dei dati, assicurata dall'art. 20 del Reg. 679/2016 (GDPR)[8].

Com'è noto, ai sensi di tale articolo, ove la base giuridica del trattamento sia il consenso o il contratto[9], e il trattamento sia effettuato con mezzi automatizzati, l'interessato ha diritto di ricevere i propri dati in formato strutturato, di uso comune e leggibile da dispositivo automatico, così come di trasmetterli ad altro titolare del trattamento, diverso rispetto a quello che li ha inizialmente raccolti e trattati, senza che quest'ultimo possa addurre impedimenti. Ancora, l'art. 20 cit. assicura all'interessato anche il diritto di ottenere la trasmissione diretta dei dati personali dal primo titolare dei dati ad altro titolare, sempreché ciò sia tecnicamente fattibile.

L'idea di fondo del legislatore europeo, nell'introdurre il diritto alla *data portability*, è stata, in primo luogo, quella di attribuire un maggior potere di controllo in capo all'interessato, consentendogli di ottenere dati in formato strutturato, di uso comune, leggibili da dispositivo automatico e, dunque, dati immediatamente (ri)usabili. Altro obiettivo è stato altresì quello di eliminare – o comunque arginare – l'effetto di dipendenza tecnologica dell'interessato dal titolare del trattamento (c.d. effetto *lock-in*), generalmente riscontrabile nella prassi. Inoltre, l'introduzione di tale innovativo diritto era ricollegato con l'idea di poter favorire la circolazione dei dati nel mercato europeo e il loro riuso, incoraggiando anche le dinamiche concorrenziali tra diversi fornitori di servizi, dato che l'interessato può chiedere a un fornitore (titolare del trattamento) che i dati personali da questi trattati siano trasferiti ad un fornitore concorrente (nella veste di altro titolare del trattamento), il quale potrà dunque subentrare agevolmente al primo nella fornitura di un servizio, analogamente a quanto sperimentato in altri settori commerciali[10].

Tale diritto ha avuto tuttavia un'applicazione ulteriore, di maggior impatto sul mercato, proprio nella sua intersezione con il fenomeno dell'intermediazione dei dati. Al di là delle originarie aspettative del legislatore europeo, infatti, il diritto alla portabilità di cui all'art. 20 GDPR, pima ancora dell'emanazione del *Data Governance Act*, ha contribuito alla nascita e all'affermazione di nuovi *player* operanti sui *data markets*: gli "intermediari di dati", ovvero i fornitori dei servizi di *data intermediation*.

Il loro rilevante ruolo strategico, manifestatosi nella prassi, ha successivamente indotto la Commissione europea a prendere in considerazione tali

7. *Ibidem*.
8. Per un commento all'art. 20 GDPR si veda Troiano 2019.
9. Ci si riferisce, segnatamente, alle condizioni di liceità di cui all'art. 6, par. 1, lett. a), e 9, par. 2, lett. a), nonché all'art. 6, par. 1, lett. b), GDPR.
10. Si pensi, a titolo meramente esemplificativo, alla portabilità del mutuo e alla portabilità dei numeri di cellulare tra operatori telefonici diversi.

operatori nella Comunicazione del 2020 dedicata alla *Strategia europea per i dati*[11], portando l'Ue a varare, successivamente, la disciplina normativa sulla governance europea dei dati[12] e l'ulteriore regolamentazione di settore, inclusa quella sugli spazi di condivisione dei dati sanitari[13], nelle quali l'intermediazione dei dati è tassello fondamentale dell'impianto regolatorio[14].

Prima ancora della disciplina giuridica europea in tema di fornitura dei servizi di intermediazione dei dati – avutasi con il *Data Governance Act* – l'operatività dei *data intermediaries* trovava una disciplina nell'ambito del Regolamento europeo sui dati personali, volto non solo a fornire un sistema di protezione agli interessati, ma anche a garantire la libera circolazione di tali dati nel mercato europeo. Sicché, facendo leva sulla liceità delle finalità del trattamento dei dati personali nell'attività di intermediazione[15] e sull'art. 20 in tema di *data portability*, sono state avanzate richieste, da parte di Hoda e per conto dei propri clienti, ad una serie di operatori commerciali della grande distribuzione e ai *big player* del settore tecnologico – Google *in primis* – ottenendo, dai propri interlocutori, forti resistenze sul mercato, proprio a causa dell'incidenza del diritto alla portabilità sul mercato dei dati e sulle dinamiche concorrenziali. Le resistenze sono sfociate *sia* in procedimenti innanzi al *Garante per la protezione dei dati personali*, che gli operatori della grande distribuzione hanno intentato nei confronti dell'intermediario, al fine di paralizzare la sua richiesta volta ad ottenere l'intero patrimonio informativo sui dati relativo ai singoli clienti, esercitata dall'intermediario medesimo per conto degli interessati in esercizio del diritto alla portabilità dei dati, *sia* in un procedimento innanzi all'*Autorità Garante per la Concorrenza e il Mercato* (AGCM), questa volta per iniziativa dell'intermediario, che lamentava una condotta anticoncorrenziale di Google volta ad ostacolare il flusso di dati richiesto da Hoda per conto dei propri clienti[16].

Sul fronte concorrenziale la minaccia percepita sul mercato dagli operatori era chiara: un nuovo *player*, l'intermediario, senza alcuno sforzo in termini di raccolta del dato, facendo valere la portabilità in nome e per conto dei propri clienti, avrebbe accumulato in un batter d'occhio e senza investimenti iniziali sui propri server quell'insieme molteplice di dati che, con grande dispendio di energie e risorse, gli operatori avevano faticato ad avere per le proprie esigenze di mercato: si pensi agli investimenti in termini di tecnologie di raccolta dei dati, al tempo prolungato per ottenerli in quantità e qualità significativa per impieghi commerciali ed industriali, e così via. L'intermediario invece, attraverso l'art. 20 GDPR, a semplice richiesta, otterrebbe per conto degli interessati, la disponibilità di tutte quelle informazioni che i diversi operatori hanno raccolto nel tempo, nell'ambito delle loro attività.

Non solo.

L'intermediario è in grado di raccogliere, sui propri server, in corrispondenza di ciascun interessato e sempre per suo conto, una quantità di gran lunga maggiore di dati rispetto al titolare del trattamento originario, in quanto accentrerebbe su di sé, per ciascun cliente-interessato, i dati personali provenienti da una pluralità di operatori. Si pensi ad esempio alla possibilità che l'intermediario ha, tramite l'esercizio del diritto alla portabilità

11. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, *Una strategia europea per i dati*, del 19 febbraio 2020, COM(2020) 66.
12. Cfr. 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 – *Data Governance Act*). Per un commento a tale regolamento cfr. Morace Pinelli 2024.
13. Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio, dell'11 febbraio 2025, sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847 (Regolamento EHDS). Per una disamina delle questioni giuridiche relative a tale regolamento si veda lo studio monografico di Faillace 2025, nonché l'opera collettanea di Morace Pinelli 2025.
14. Sul rapporto tra intermediazione di dati e diritto alla portabilità nel settore sanitario, con particolare riferimento agli spazi di condivisione dei dati sanitari disciplinati nel Regolamento EHDS si veda Bravo 2025.
15. In tema di diritto a trattare dati personali nello svolgimento dell'attività economica v., *amplius*, Bravo 2018.
16. Si veda, per i procedimenti innanzi ad entrambe le *Authority*, quanto illustrato *infra*, nel prosieguo del discorso.

su delega dell'interessato, di concentrare, per ogni *data subject*, dati provenienti da titolari diversi, come ad esempio i dati gestiti dai singoli *Internet Service Providers* (Google, Meta, Apple, Amazon, Booking, ecc.) con cui l'utente si relaziona, i dati accumulati nelle "carte fedeltà" dei diversi distributori sul mercato (ad esempio le carte fedeltà dei grandi magazzini, dei supermercati, delle catene di distribuzione di libri, ecc.), oltre, eventualmente, a dati di altro tipo come quelli bancari, sanitari e quant'altro il singolo interessato voglia far confluire nell'intermediario. Il senso dell'operazione è, per l'interessato, quello di riappropriarsi del controllo sui propri dati e della loro gestione, tramite l'ausilio di un soggetto che professionalmente agirà per valorizzarli anche in prospettiva di mercato, traendo benefici per l'interessato e trattenendo una quota ridotta per il servizio di intermediazione fornito.

Il *data subject*, generalmente, vede i propri dati raccolti in grande quantità da operatori di mercato senza tuttavia poterne avere il controllo e senza poter ottenere benefici diretti o indiretti dal loro utilizzo, salvo eventualmente trascurabili "concessioni", come sconti di modesta entità, piccole donazioni di prodotti o fornitura senza controprestazioni in denaro, più che ripagate in realtà dall'accumulo di dati da utilizzare sui mercati secondari[17]. Con l'attività svolta dall'intermediario, in qualche modo, l'interessato interagisce con l'intermediario, che ha competenze tecnico-giuridiche per acquisire i dati da altri titolari del trattamento, restituire governance e controllo all'interessato sui propri dati e concordare con quest'ultimo le modalità di utilizzo e i benefici negoziabili.

In altre parole, l'intermediario finisce per costituire dei "super-profili" degli interessati, per loro conto, da gestire in maniera profittevole o comunque vantaggiosa nei rapporti con altri soggetti terzi, secondo modalità di riuso da programmare, riversando sugli interessati i vantaggi (economici e non) ottenuti dal *secondary use* di tali dati, trattenendo al contempo, in logica *win-win*, una parte che costituisce il margine di profitto per l'intermediazione professionale svolta. Al contempo, l'intermediario agisce ne superiore interesse dell'interessato, che deve essere sempre fatto salvo[18].

Si comprendono bene le resistenze degli operatori di mercato nei confronti degli intermediari, così come le strategie dell'Ue nel valorizzarli, sul piano degli intenti normativi di regolazione del mercato. La fornitura dei servizi di intermediazione, infatti, consente a imprese anche di piccole dimensioni, come start-up nel settore high-tech, di competere rapidamente anche con i più consolidati giganti attivi da tempo sul medesimo settore: le imprese europee, in tal modo, finiscono per avere l'occasione di recuperare fette di mercato nei *digital markets*, ipercontrollati dalle multinazionali soprattutto americane in regime di oligopolio, se non di pressoché sostanziale monopolio – o quasi – nei sottoinsiemi in cui i mercati digitali trovano esplicazione[19].

2.3. Segue: La portabilità dei dati e la questione della delega

L'avvento degli intermediari di dati, sul piano giuridico, è stato possibile sotto l'egida del GDPR mediante l'uso congiunto di due strumenti giuridici: il *diritto alla portabilità* di cui all'art. 20 e la *delega* dell'interessato all'intermediario, che consentisse a quest'ultimo di agire per conto del primo, al fine di richiedere ed ottenere i dati personali da utilizzare per ulteriori finalità.

Seppur con talune differenze da intermediario a intermediario, lo schema operativo generalmente applicato prevede i seguenti *step*: (i) l'intermediario, in fase di contrattualizzazione del rapporto con il proprio cliente, interessato al trattamento di dati posto in essere da un soggetto terzo, titolare del trattamento e fornitore di servizi, si fa conferire la delega per l'esercizio del diritto alla portabilità nei confronti di quest'ultimo; (ii) ottenuta la delega, l'intermediario richiede al titolare del trattamento, per conto dell'interessato, il trasferimento

17. Quanto ai *two-sided markets* con riferimento ai mercati di dati si veda Zeno Zencovich 2019.
18. Cfr. art. 12, par. 1, lett. m), del DGA, ai sensi del quale " il fornitore di servizi di intermediazione dei dati che offre servizi agli interessati agisce nell'interesse superiore di questi ultimi nel facilitare l'esercizio dei loro diritti, in particolare informandoli e, se opportuno, fornendo loro consulenza in maniera concisa, trasparente, intelligibile e facilmente accessibile sugli utilizzi previsti dei dati da parte degli utenti dei dati e sui termini e le condizioni standard cui sono subordinati tali utilizzi, prima che gli interessati diano il loro consenso".
19. Si pensi ad Amazon per il commercio elettronico diretto, a Google per i motori ricerca, ecc.

diretto dei dati presso di sé, mettendoli a disposizione dello stesso interessato per successivi utilizzi; (iii) l'intermediario reitera le richieste verso altri titolari del trattamento, fornitori di servizi, collazionando ulteriori dati presso di sé per conto dell'interessato, mettendoglieli a disposizione; (iv) d'accordo con il cliente-interessato, l'intermediario attiva strategie di valorizzazione, ovvero di riuso, dei dati personali con soggetti terzi (*data users*), a beneficio anche dei medesimi interessati, in una logica "*win-win*", ottenendo remunerativitá e altri vantaggi, con trattenimento di una quota concordata con i propri clienti (ad esempio, 10%) quale commissione per l'attività di intermediazione.

Generalmente l'intermediario, acquisiti i dati da un certo numero di clienti-interessati, rende accessibile ai *data users* – incluso pubbliche amministrazioni, università, imprese, enti non lucrativi – l'insieme di tali dati (o una parte di essi) in forma aggregata ed anonimizzata, per analisi statistiche, scientifiche o di mercato. A ben guardare, attraverso l'uso congiunto della portabilità dei dati e della delega, gli aspetti innovativi che sono emersi nella prassi, già richiamati sopra e qui di seguito ricapitolati, sono almeno tre:

(i) per un verso si è avuta l'affermazione di nuovi *player* europei, in un mercato dominato dalle multinazionali straniere, soprattutto americane, nel quale l'intermediario, dotato di mezzi e know-how adeguati, riesce ad acquisire con una certa facilità e senza eccessivi sforzi, da una pluralità di titolari del trattamento e fornitori di servizi, i dati personali che questi ultimi hanno raccolto nel tempo con ingenti risorse e che ora, in tal modo, cumulati, ritornano (anche) nella disponibilità degli stessi interessati;

(ii) per altro verso si è avuta anche l'emersione del ruolo attivo, potenzialmente tutorio, dell'intermediario di dati, che, agendo per conto dell'interessato e meglio attrezzato di quest'ultimo, può assisterlo nell'esercizio dei diritti e nella cura dei suoi interessi;

(iii) v'è poi da considerare anche la (parziale) effettiva riappropriazione di poteri e facoltà, da parte degli interessati, sui propri dati personali, grazie all'azione svolta dall'intermediario. Gli interessati, grazie a tale nuovo *player* ed all'utilizzo della *data portability*, ottengono la disponibilità dei propri dati collazionandoli da sorgenti e fornitori diversi, con la possibilità di negoziare in proprio favore, tramite la capacità dell'intermediario, l'utilizzo secondario dei dati personali che intendono veicolare a soggetti terzi, nelle forme adeguate a garantire la loro tutela. Generalmente i *providers*, nel fornire i diversi servizi (navigazione online, social network, motori di ricerca, mappe satellitari e geolocalizzazione, ecc.), raccolgono una grande mole di dati che riutilizzano a proprio vantaggio in un mercato secondario di dati, da cui l'interessato viene estromesso, lasciandogli, quale esclusivo beneficio, il solo servizio con cui viene acquisita la disponibilità materiale dei dati[20]. L'intervento dell'intermediario, viceversa, consente all'interessato, suo tramite, non solo di riottenere la disponibilità materiale di quei dati, "rastrellandoli" da una molteplicità di provider titolari del trattamento e concentrandoli in un unico contesto, ma anche di riappropriarsi delle possibilità di governance del loro utilizzo secondario, possibile proprio grazie alla capacità tecnica dell'intermediario. In tal modo si può rendere effettiva quell'*autodeterminazione informativa*, da cui l'interessato finiva per essere "espropriato" e di cui ora, grazie al ruolo dell'intermediario, riesce a "riappropriarsi".

Accanto alle evidenti potenzialità dell'intermediazione dei dati v'è anche qualche preoccupazione, dovuta sia al quadro regolamentare ancora incerto ai tempi dell'emanazione e della prima applicazione del GDPR su tale specifica materia, sia ai potenziali nuovi rischi che possono emergere dal fenomeno in esame, non adeguatamente ponderati in sede di emanazione del Regolamento sulla data protection.

Il Garante per la protezione dei dati personali, in Italia, ha iniziato a prendere cognizione del fenomeno al momento di prima emersione delle segnalazioni proprio sull'operato di Hoda, alle prese con il suo servizio di punta denominato "Weople", segnalazioni inoltrate nei primi mesi del 2019 da operatori della grande distribuzione commerciale: questi ultimi, nella loro qualità di titolari del trattamento, si erano visti rivolgere numerose richieste di portabilità dei dati dal predetto intermediario, per delega dei propri clienti, secondo lo schema di operatività sopra richiamato e, dubitando della liceità dell'operazione, tra l'altro non

20. Zeno Zencovich 2018; Resta-Zeno Zencovich 2018.

gradita, l'avevano prontamente segnalata all'Autorità di settore[21].

Il Garante per la protezione dei dati personali, sotto la presidenza di Antonello Soro, avviata l'istruttoria, decideva di interessare della questione l'EDPB, ritenendo che il tema fosse di interesse europeo e non esclusivamente nazionale. Nella nota di trasmissione al Comitato europeo veniva evidenziato che "si tratta di una *questione molto rilevante* che, pur venuta in evidenza in Italia, impone una riflessione generale che *non può essere rimessa alle singole autorità di protezione dati*. Il caso riguarda l'*applicazione del diritto alla portabilità* dei dati: un'impresa italiana si è infatti proposta come intermediaria nel rapporto fra titolari ed interessati chiedendo, *su delega* di questi ultimi, di ottenere le informazioni personali custodite presso importanti soggetti imprenditoriali, in particolare nel settore della grande distribuzione al fine di riunirle all'interno di una propria banca dati da sottoporre ad *enrichment*. Il tema è dunque legato alla '*commerciabilità*' dei dati, con l'ulteriore complicazione dell'esercizio per delega del diritto ed il conseguente non remoto rischio di possibili duplicazioni delle banche dati oggetto di portabilità"[22].

La discussione innanzi all'EDPB non sarebbe stata affrontata dal Collegio presieduto da Antonello Soro, per via della scadenza del mandato. Nel Comunicato stampa relativo a tale questione, il Garante chiariva comunque che "(…) attenderà dunque il parere dell'EDPB per concludere l'istruttoria"[23] e che "nel frattempo, i soggetti privati che riceveranno le richieste di portabilità dei dati da parte (…) [dell'intermediario] dovranno operare nel rispetto del principio di accountability stabilito dal Regolamento Ue e valutare se ottemperare alle richieste o motivare un eventuale rifiuto"[24].

Nell'attesa, il Garante – anche per via della prossima scadenza del mandato – rinunciava dunque a prendere espressamente una propria posizione,

21. La ricostruzione della vicenda e le sfumature contenute nella richiesta di parere che il Garante ha avanzato all'EDPB sono state esplicitate nel Comunicato stampa del 1° agosto 2019, doc. web n. 9126709, nel quale si legge che "Con una lettera a firma del Presidente Antonello Soro, l'Autorità Garante per la privacy ha posto all'attenzione del Comitato europeo per la protezione dei dati personali (EDPB) la questione relativa a 'Weople', l'*app* che promette ai propri iscritti una remunerazione in cambio della cessione dei loro dati personali. A partire dai primi mesi del 2019 sono state diverse le segnalazioni giunte all'Autorità da parte di imprese della grande distribuzione che lamentavano di aver ricevuto da parte di 'Weople' numerosissime richieste di trasferire alla piattaforma dati personali e di consumo registrati nelle carte di fedeltà. L'impresa italiana, che gestisce la *app* e offre servizi di vario genere (offerte commerciali, analisti statistiche e di mercato), si propone infatti come intermediaria nel rapporto tra aziende e utenti chiedendo, su delega di questi ultimi, di ottenere le informazioni personali custodite presso grandi imprese allo scopo di riunirle all'interno della propria banca dati. L'attenzione del Garante si è concentrata, in particolare, sulla corretta applicazione, da parte della società, del cosiddetto diritto alla '*portabilità dei dati*' introdotto dal nuovo Regolamento europeo, con l'ulteriore *complicazione* determinata dall'*esercitare tale diritto mediante una delega* e con il conseguente *rischio di possibili duplicazioni* delle banche dati oggetto di portabilità. L'altro aspetto segnalato dal Garante nella lettera riguarda il delicato tema della '*commerciabilità' dei dati*, causata dall'attribuzione di un vero e proprio *controvalore al dato personale*. Su entrambe le questioni, il Garante ha dunque chiesto al Comitato, che riunisce tutte le Autorità Garanti dell'Unione, di pronunciarsi. L'attività di 'Weople', scrive il Garante, 'può produrre effetti in più di uno Stato dell'Unione' in ragione delle richieste di portabilità che potranno essere avanzate e delle questioni relative alla 'valorizzazione economica dei dati personali ed alla natura 'pro-concorrenziale' del diritto alla portabilità'. Per questi motivi, pur essendo emerso in Italia, il caso della *app* impone, ad avviso del Garante, una riflessione generale che è più opportuno condividere con le altre Autorità di protezione dati. Il Garante attenderà dunque il parere dell'EDPB per concludere l'istruttoria avviata sulla *app* (…)".
22. Lettera del Presidente del Garante per la protezione dei dati personali al Presidente dell'*European Data Protection Board* (EDPB), avente ad oggetto *Richiesta di parere in tema di commercializzazione dei dati personali e diritto alla portabilità* (Garante per la protezione dei dati personali, doc. web n. 9126725 del 1° agosto 2019. Si veda anche, di ugual tenore, il Comunicato Stampa del 1° agosto 2019, cit.
23. GPDP, Comunicato stampa del 1° agosto 2019, cit.
24. *Ibidem*.

così come a fornire indicazioni agli operatori, lasciandoli di fatto "soli" di fronte ai nuovi problemi applicativi sollevati dalla prassi, nell'attesa di un intervento di respiro europeo.

L'esperienza significativa sul caso Weople, tuttavia, ha alimentato un confronto anche su altri tavoli, in quanto è stata oggetto di disamina anche nell'ambito dell'*Indagine conoscitiva sui Big Data*, condotta congiuntamene dal Garante per la protezione dei dati personali, dall'Autorità Garante per la Concorrenza e il Mercato (AGCM) e dall'Autorità per le Garanzie nelle Comunicazioni (AGCOM). In tale indagine, il confronto tra le tre autorità aveva portato a valutare positivamente il *business model* adottato per la fornitura del servizio di *data intermediation*, basato sull'esercizio del diritto alla portabilità dei dati accompagnato dal conferimento della delega all'intermediario. Ciò in quanto "Tali iniziative [di *data intermediation*] potrebbero fungere da strumento di *consumer empowerment* potenzialmente in grado di superare in parte le descritte limitazioni derivanti dall'attuale disciplina del diritto alla portabilità dei dati, in termini di contribuzione alla costruzione di una consapevolezza da parte degli utenti circa il valore economico dei loro dati personali, grazie all'ottenimento di una remunerazione per l'utilizzo di tali dati da parte di soggetti terzi"[25].

Poco dopo, proprio sul servizio Weople fornito da Hoda, s'è pronunciata anche l'AGCM, che, nel 2022, ha accolto le rimostranze da questa avanzate nei confronti di Google, là dove, in chiave anticoncorrenziale, appariva restia ad adeguare i propri sistemi informatici per favorire le richieste di portabilità avanzate dall'intermediario, su delega dei propri clienti[26].

25. GPDP-AGCM-AGCOM, *Indagine conoscitiva sui Big Data*, Rapporto finale, 10 febbraio 2020, disponibile online, doc. web n. 9264297, p. 99. Ivi le Autorità, nella rassegna in tema di *data portability*, hanno evidenziato che "(…) esempi di strumenti di portabilità dei dati attraverso un mezzo automatizzato (generalmente *app*) vengono, *inter alia*, dall'Italia, dove sono stati sviluppati sistemi che consentono agli utenti di richiedere a diversi titolari di trattamento l'estrazione dei propri dati personali e di archiviarli in un'area dedicata (ad esempio, Weople). Con l'inserimento dei dati personali nell'area dedicata l'utente riceve una remunerazione, che deriva dai pagamenti che i titolari di trattamento effettuano per avere degli spazi pubblicitari all'interno di dette aree e per la mera lettura delle offerte commerciali da parte degli utenti destinatari (c.d. mercato dell'attenzione). I dati presenti nelle aree dedicate possono essere, peraltro, ulteriormente elaborati tramite un'attività di profilazione. Successivamente i risultati di tali attività verrebbero venduti alle imprese interessate alla loro acquisizione, anche in questo caso per lo svolgimento campagne pubblicitarie e/o offerte commerciali personalizzate, generando per gli utenti ulteriori fonti di remunerazione dell'utilizzo dei dati personali degli utenti medesimi". Ovviamente la destinazione di tali dati per l'uso secondario può ben riguardare il settore della ricerca scientifica, come ad esempio avviene nell'ambito del Progetto UE Next Generation PNRR PE09 "GRINS – *Growing Resilient, Inclusive and Sustainable*".

26. Cfr. provvedimento dell'AGCM del 5 luglio 2022, di avvio dell'istruttoria, reso nei confronti di Google LLC, su segnalazione di Hoda S.r.l., società italiana attiva nell'intermediazione di dati personali attraverso l'*app* denominata "Weople", seguito dal provvedimento dell'AGCM del 18 luglio 2023, di chiusura dell'istruttoria, con interventi di Mediaset Spa, Computer & Communications Industry Association, Associazione Italiana Internet Provider (AIIP) ed Altroconsumo. Il procedimento era nato a seguito delle lamentele di Hoda in ordine alla condotta asseritamente anticorrenziale di Google, che avrebbe frapposto ostacoli tecnici alla portabilità dei dati richiesti da Hoda per conto dei propri clienti, al fine del loro riuso anche in ambito commerciale. A pag. 4 (par. 9) del provvedimento del 2023 l'AGCM afferma che "La condotta contestata a Google, nel pregiudicare l'esercizio, da parte dell'utente finale, del diritto alla portabilità dei propri dati stabilito dall'articolo 20, comma 2, del GDPR, si risolve in un indebito sfruttamento, da parte della stessa Google, dei consumatori finali nella misura in cui determina una limitazione dei benefici che i consumatori potrebbero trarre dalla valorizzazione dei loro dati personali. Tale condotta presenta un ulteriore carattere restrittivo della concorrenza nella misura in cui limita la possibilità di operatori alternativi a Google di sviluppare forme innovative di utilizzo dei dati personali. In particolare, Hoda ha rappresentato gli effetti negativi della condotta di Google sulla sua iniziativa volta a sviluppare, attraverso la piattaforma Weople, una innovativa attività commerciale, consistente nel valorizzare i dati personali con l'autorizzazione del suo titolare in prospettive merceologiche ancora inesplorate, con particolare

Da ultimo, alla fine del 2024, il Garante è ritornato ad occuparsi ancora una volta del caso Weople, in altro procedimento, con istruttoria avviata nel 2021, in base a segnalazioni e reclami provenienti prevalentemente da aziende della grande distribuzione, culminato con provvedimento n. 704 del 14 novembre 2024 doc. web n. 10108848[27].

Le questioni affrontate in tale provvedimento sono molteplici, tra cui: (i) l'individuazione della corretta base giuridica del trattamento posto in essere dall'intermediario, anche con riguardo al trattamento concernenti minori; (ii) l'inclusione, nella valutazione di impatto di cui all'art. 35 GDPR, delle ripercussioni che la commercializzazione dei dati ha sulla libera prestazione del consenso al trattamento dei dati e le misure da adottare per preservare tale libertà; (iii) il meccanismo di delega per l'esercizio dei diritti dell'interessato, incluso il diritto alla portabilità dei dati e i limiti alla sua estensione. Rimandando ad altra sede una più dettagliata analisi dell'intero provvedimento, ai fini del discorso che si sta conducendo mi preme rimarcare i significativi passaggi argomentativi sul rapporto tra delega ed esercizio del diritto dell'interessato alla portabilità dei dati.

Il Garante, con il provvedimento ad esame, s'è pronunciato sia nel senso dell'ammissibilità della delega per l'esercizio dei diritti dell'interessato, sia nel senso che la medesima possa essere rivolta ad una persona giuridica, ma ha rimarcato anche che, nel peculiare contesto del trattamento dei dati personali, l'ammissibilità di principio, sul piano giuridico, si accompagna con l'individuazione di requisiti rigorosi, volti ad accertare che la manifestazione di volontà dell'interessato sia specifica ed inequivoca e tale da circoscrivere l'operatività del rappresentante sia sul piano oggettivo che su quello temporale, non potendosi ritenere accettabile, nella materia *de qua*, una delega generale e *sine die*[28].

Per il Garante, nel provvedimento citato, la delega all'intermediario è dunque ammissibile, anche se è persona giuridica, ma deve riferirsi "ad un *singolo atto* – o ad una *serie predeterminata di atti* – di esercizio dei diritti nei confronti del titolare originario" e *non* può essere "utilizzata *illimitatamente e fino a 'revoca'* (…) in ragione delle esigenze legate allo sfruttamento commerciale dei dati personali dell'interessato"[29].

La delega in altre parole, come argomentato dall'Autorità, eredita le caratteristiche dell'atto delegato e ciò conduce all'individuazione di limiti, desumibili dal sistema anche se non esplicitati sul piano normativo, che segnano i confini stessi della sua ammissibilità. Sul punto, infatti, il Garante ha affermato che "Nel caso in argomento, (…) la medesima esigenza che la delega per l'esercizio del diritto alla portabilità assuma le caratteristiche dell'atto delegato (sia quindi *contenuta in un documento che si riferisca ad una o più specifiche attività* il cui *oggetto è compiutamente definito* e possa prevedere la *reiterazione di tali attività solo se espressamente menzionata*) rappresenta, *in virtù del rango dei diritti oggetto di tutela, un requisito minimo* sia per garantire agli interessati un reale ed effettivo controllo sul trattamento dei propri dati personali, sia per consentire al titolare originario

riferimento al contesto geografico nazionale". Nel corso del procedimento Google presentava, ai sensi della disciplina antitrust, una serie di impegni per far venir meno i profili anticoncorrenziali emersi in sede istruttoria, che l'*Authority* considerava idonei e rendeva conseguentemente obbligatori nei confronti di Alphabet Inc., Google LLC, Google Ireland Limited e Google Italy Srl.

27. Non è chiaro, in realtà, se si tratti dell'epilogo della vicenda per la quale c'era stato l'interessamento dell'EDPB, in seguito dell'originaria istruttoria, o se si tratti di procedimento riavviato *ex novo*, sulla base di altre segnalazioni pervenute all'Autorità, in nuova composizione. Nel provvedimento tale aspetto non viene chiarito esplicitamente.

28. Nel provvedimento n. 704 del 14 novembre 2024, doc. web n. 10108848, il Garante per la protezione dei dati personali chiarisce che "Con riferimento alla *delega avente ad oggetto l'esercizio dei diritti dell'interessato* e, in particolare, il *diritto alla portabilità* è stato osservato nell'atto di avvio del procedimento amministrativo che la stessa, dovendo avere quantomeno i *requisiti* degli atti che si intendono compiere in rappresentanza dell'interessato, dovrebbe essere indicatrice di una *volontà specifica e inequivoca dell'interessato* stesso, *circoscrivendo l'operatività del delegato sia dal punto di vista oggettivo che temporale*".

29. *Ibidem*.

di comprovare l'inequivoca volontà dei soggetti che intendono esercitare i propri diritti".

Altro problema riguarda l'estensione della delega e, in particolare, se la medesima possa concernere anche la revoca del consenso. Il Garante la esclude in considerazione della collocazione sistematica dell'art. 7 GDPR, in cui la revoca del consenso al trattamento dei dati personali trova la sua disciplina, nella parte dedicata alle condizioni di liceità del trattamento e non all'esercizio dei diritti dell'interessato, disciplinati agli artt. 12-23 GDPR. Meno condivisibile risulta invece l'assunto, contenuto del provvedimento in parola, secondo cui il consenso al trattamento sarebbe da ritenersi "atto personalissimo": come s'è già avuto modo di rilevare[30], lo stesso GDPR, all'art. 8, prevede che, qualora il consenso non possa essere prestato direttamente dal minore per via dei limiti ivi delineati, viene manifestato da coloro che esercitano la responsabilità genitoriale e che ne hanno dunque la rappresentanza *ex lege*[31].

È utile ripercorrere *verbatim* il passaggio argomentativo rinvenibile nel provvedimento citato, nel quale, con riguardo al tema ora in parola, si trova annotato che, "Quanto alla delegabilità della revoca del consenso, invece, si prende atto delle argomentazioni difensive tendenti a ricondurre tale azione nell'alveo dei diritti di cui agli artt. 15-22 del Regolamento e a consentirne la delegabilità. Tuttavia, deve confermarsi quanto osservato nell'atto di avvio del procedimento amministrativo, e cioè che la collocazione della previsione della facoltà di revoca del consenso nell'ambito dell'art. 7 del Regolamento ha una ragione sistematica ben chiara, e cioè quella di equiparare i connotati e gli effetti della dichiarazione di volontà negativa in ordine allo svolgimento dei trattamenti a quelli della dichiarazione di volontà positiva, sia con riferimento alle forme di espressione che agli effetti. Da questo punto di vista l'istituto del consenso rappresenta ormai *atto personalissimo*, nonché lo strumento di garanzia del diritto fondamentale in grado di realizzare l'autodeterminazione informativa (l'art. 8 della Carta dei diritti fondamentali dell'Unione europea lo parifica alla riserva di legge) e non può, per tale ragione, essere ridotto ad atto dispositivo *stricto sensu* delegabile in grado di vanificare il contenuto stesso del diritto chiamato a garantire. Ricondurre la volontà di revoca del consenso nell'ambito dell'esercizio dei diritti dell'interessato, oltre a non trovare riscontro nelle disposizioni normative, sottrarrebbe all'interessato quella facoltà di espressione diretta e anche semplificata della propria volontà (in linea con il consenso precedentemente acquisito) di interrompere con effetto immediato il trattamento, determinando un ingiustificato disallineamento fra consenso e revoca, a tutto danno proprio dell'interessato"[32].

Si tratta di osservazioni che, seppur vagliabili criticamente, non possono essere trascurate neanche con riguardo ai servizi di delega che dovranno essere approntati per gli spazi di condivisione di dati, previsti dal Regolamento EHDS, la cui definizione è rimessa al legislatore nazionale.

2.4. L'attenzione dell'Ue per il fenomeno dell'intermediazione dei dati come fattore di sviluppo e la regolamentazione del mercato. L'intermediazione dei dati nel *Data Governance Act*

S'è visto come le iniziali preoccupazioni del Garante sul fronte domestico relative alla prima istruttoria del 2019 sul caso Hoda non siano sfociate, nell'immediatezza, in un'azione repressiva o sanzionatoria del fenomeno, né in altri interventi connotati dall'applicazione del meccanismo di cooperazione tra le diverse autorità di controllo nazionali, né, ancora, hanno dato adito ad interventi, anche solo di soft law, da parte dell'EDPB o dell'EDPS, nonostante le sollecitazioni della *Data Protection Authority* nostrana.

Una prima significativa risposta istituzionale a tale sollecitazioni sembra sia pervenuta sia con la Comunicazione della Commissione sulla *Strategia europea dei dati*, già citata, significativamente resa nel 2020, sia, in via legislativa, con

30. Cfr. Bravo 2017; Bravo 2019.

31. Ciò esclude, evidentemente, la natura di "atto personalissimo" del consenso, essendo altrimenti precluso al genitore o al tutore il compimento dell'atto per conto del minore, come ad esempio avviene in caso di riconoscimento del figlio naturale.

32. Garante per la protezione dei dati personali, Provvedimento n. 704 del 14 novembre 2024, doc. web n. 10108848, cit.

l'emanazione del *Data Governance Act*[33], ove, in linea con una progettualità delineata mediante la predetta Comunicazione, s'è provveduto a disciplinare il fenomeno della *data intermediation* agendo su tre piani distinti, che configurano tre diversi modelli di intermediazione:

(i) v'è il modello di intermediazione di dati affidato ai "*fornitori dei servizi di intermediazione dei dati*", ossia a soggetti che operano per scopi commerciali, raccogliendo dati provenienti da interessati e *data holders*, per renderli disponibili a terzi (*data users*), rispettivamente con il consenso degli interessati medesimi o con l'autorizzazione dei *data holders*, nel rispetto delle condizioni di liceità indicate dal GDPR[34]. Si tratta di attività di intermediazione che può essere svolta in forma tradizionale, mettendo in relazione soggetti estranei all'intermediario, oppure in forma *cooperativa*, mediante vere e proprie cooperative di dati[35], ove l'intermediario è soggetto che aggrega dati conferiti dai propri "membri" – generalmente "soci" della cooperativa di dati – che mantengono il controllo e la gestione dell'ente[36]. L'intermediario è tenuto a notificare all'autorità competente (l'AgID, per l'Italia) l'intenzione di svolgere la propria attività di fornitore di servizi di intermediazione dei dati, rispettare determinate condizioni di mercato, previste dall'art. 12 del DGA, rimanendo soggetto all'azione di controllo della predetta *Authority*. Il modello di intermediazione ivi delineato impone al fornitore di agire in posizione neutrale, senza utilizzare per sé i dati personali nei cui confronti si pone come intermediario, ma assicurando comunque il perseguimento del superiore interesse degli interessati. Sicché questi ultimi, soprattutto in caso di cooperative di dati, si trovano di fronte ad un soggetto che supporta gli interessati nella selezione dei dati da condividere (e di quelli da escludere dalla condivisione), nell'esercizio dei propri diritti e nella negoziazione dei vantaggi a proprio favore, portando ad un rafforzamento significativo della posizione dell'interessato, su quello economico relativo alla posizione (di forza) sul mercato e sul piano giuridico[37];

(ii) v'è altresì il modello di *data intermediation* altruistico, affidato alle organizzazioni per l'altruismo dei dati, che si indirizza al soddisfacimento di obiettivi di interesse generale, inclusa l'assistenza sanitaria[38]. È una declinazione in

33. Per un commento al *Data Governance Act* si veda Morace Pinelli 2024.

34. Sull'intermediazione di dati, in particolare sulle connessioni che a tal riguardo si hanno tra il GDPR e il *Data Governance Act*, si veda Bravo 2020; Bravo 2021; Poletti 2022; Resta 2022; Resta-Zeno Zencovich 2023; Morace Pinelli 2024.

35. In tema di cooperative di dati, disciplinate nel *Data Governance Act*, si veda Bravo 2023; Petrone 2023; nonché i contributi raccolti all'esito del progetto di terza missione dell'Università di Bologna in materia di Cooperative di dati, nel volume curato da Bravo 2024.

36. All'art. 2, par. 1, n. 15, del DGA si trova la definizione di "servizi di cooperative di dati", intesi quali "servizi di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di *aiutare i propri membri nell'esercizio dei loro diritti* in relazione a determinati dati, anche per quanto riguarda il *compiere scelte informate* prima di acconsentire al trattamento dei dati, di procedere a uno *scambio di opinioni* sulle finalità e sulle *condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati*, o di *negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri* prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali".

37. Cfr. Bravo 2023; Poletti 2024; Ricci-Spangaro 2024; nonché Cardinali 2024.

38. L'*altruismo dei dati* viene definito, all'art. 2, par. 1, n. 16, del DGA, come "la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'*assistenza sanitaria*, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione,

senso solidaristico[39] dell'attività di intermediazione commerciale sui dati, la quale ultima riemerge anche in tale settore qualora le organizzazioni per l'altruismo di dati perseguano, unitamente ad un intento altruistico-solidaristico – che dunque non è esclusivo – anche un concomitante scopo lucrativo, puntando a stabilire (anche) relazioni commerciali tra un numero indeterminato di interessati e *data holders*, da un lato, e *data users*, dall'altro lato[40];

(iii) v'è, poi, il modello di *data intermediation* affidato ad *enti pubblici*, che possono consentire il *riuso dei dati*, di cui hanno la disponibilità per fini istituzionali, mediante il consenso degli interessati ed avvalendosi di "organismi competenti", chiamati ad effettuare le operazioni tecniche necessarie per rendere disponibili i dati ai *data users*, per finalità commerciali e non commerciali, nel contesto di *ambienti controllati* e con possibilità di applicazione di tariffe *ad hoc* per garantire la sostenibilità del servizio. Il legislatore europeo non usa esplicitamente il termine "intermediazione" per il ruolo degli enti pubblici, volti a garantire il riuso dei dati personali da questi detenuti in ragione dei loro compiti istituzionali. Che di *data intermediation* si tratti, tuttavia, può essere chiaramente desunto anche nella definizione stessa di "riutilizzo", la quale, ai sensi dell'art. 2, par. 1, n. 2, del DGA, si riferisce all'"utilizzo di dati in possesso di enti pubblici da parte di persone fisiche o giuridiche a fini commerciali o non commerciali diversi dallo scopo iniziale nell'ambito dei compiti di servizio pubblico per i quali i dati sono stati prodotti, fatta eccezione per lo scambio di dati tra enti pubblici esclusivamente in adempimento dei loro compiti di servizio pubblico".

3. L'intermediazione dei dati nel settore pubblico e il *reuse of data held by public bodies*

Dunque, l'intenzione del legislatore, con la regolamentazione del riuso dei dati personali raccolti in ambito pubblico, è quella di consentirne il riuso, anche per fini commerciali, in favore di persone fisiche o giuridiche, al di fuori delle finalità istituzionali per le quali il trattamento è inizialmente avvenuto, restituendo alla collettività la possibilità di trarre conoscenza e occasioni commerciali da tali dati, con le garanzie per il rispetto della disciplina posta a protezione delle persone fisiche con riguardo ai trattamenti dei dati personali che li riguardano.

La prospettiva seguita dal legislatore europeo, per tale modello di intermediazione, è quella indicata nel considerando n. 6 del DGA, ove espressamente si enuncia che "l'idea che i dati generati o raccolti da enti pubblici o altre entità a carico dei bilanci pubblici debbano apportare benefici alla società è da tempo parte integrante delle politiche dell'Unione. La direttiva (UE) 2019/1024 e la normativa settoriale dell'Unione garantiscono che gli enti pubblici rendano facilmente disponibile per l'utilizzo e il riutilizzo una quota maggiore dei dati che producono. Spesso talune categorie di dati conservati in basi di dati pubbliche, quali dati commerciali riservati, dati soggetti a segreto statistico e dati protetti da diritti di proprietà intellettuale di terzi, compresi segreti commerciali e dati personali, spesso non sono messe a disposizione, nemmeno per attività di ricerca o di innovazione nel pubblico interesse, nonostante tale disponibilità sia possibile in conformità del diritto dell'Unione applicabile, in particolare del regolamento

della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale".

39. Quanto al principio di solidarietà si vedano le insuperabili pagine di Rodotà 2014 e di Alpa 2022. Con riguardo alla declinazione di tale principio con riguardo ai dati personali si rimanda a Bravo 2023-b; Bravo 2023-c; Bravo 2023-d.

40. Si veda, al riguardo, il tenore dell'art. 15 del DGA, rubricato "Deroghe", di chiusura del Capo III dedicato alla fornitura dei servizi commerciali di intermediazione dei dati, nel quale si trova statuito che "Il presente capo non si applica alle organizzazioni per l'altruismo dei dati riconosciute o ad altre entità senza scopo di lucro nella misura in cui le loro attività consistono nel cercare di raccogliere, per obiettivi di interesse generale, dati messi a disposizione da persone fisiche o giuridiche sulla base dell'altruismo dei dati, a meno che tali organizzazioni e entità non puntino a stabilire relazioni commerciali tra un numero indeterminato di interessati e titolari dei dati, da un lato, e utenti dei dati, dall'altro".

(UE) 2016/679 e delle direttive 2002/58/CE e (UE) 2016/680. A causa della sensibilità di tali dati, prima che essi siano messi a disposizione si devono soddisfare alcuni requisiti procedurali tecnici e giuridici al fine, se non altro, di garantire il rispetto dei diritti di terzi sui dati in questione o di limitare l'effetto negativo sui diritti fondamentali, sul principio di non discriminazione e sulla protezione dei dati. L'adempimento di tali requisiti risulta abitualmente molto dispendioso in termini di tempo e richiede un livello molto elevato di conoscenze. Ciò ha determinato un utilizzo insufficiente di tali dati. Per quanto alcuni Stati membri stiano istituendo strutture, procedure o adottando norme per agevolare tale tipo di riutilizzo, ciò non accade in tutta l'Unione. Al fine di agevolare l'utilizzo dei dati per la ricerca e l'innovazione europee da parte di soggetti pubblici e privati, sono necessarie condizioni chiare per l'accesso a tali dati e il loro utilizzo in tutta l'Unione".

Il *Data Governance Act*, per i dati appartenenti a categorie protette, incluso i dati personali, detenuti da enti pubblici, consente dunque a questi ultimi di concedere l'accesso a terzi ai fini del riuso di tali dati, anche per fini commerciali, purché ciò avvenga alle condizioni previste dall'art. 5 del predetto Regolamento, assicurando un livello di protezione conforme alla natura protetta dei dati da sottoporre a riuso. In particolare, gli enti pubblici, a fronte di una richiesta di riutilizzo dei dati, sono tenuti a concedere l'accesso per il riutilizzo dei dati soltanto qualora abbiano garantito che, a seguito della richiesta medesima, i dati siano stati anonimizzati, nel caso di dati personali, e modificati, aggregati o trattati mediante qualsiasi altro metodo di controllo della divulgazione, nel caso di informazioni commerciali riservate, compresi i segreti commerciali o i contenuti protetti da diritti di proprietà intellettuale[41]. Inoltre, gli enti interessati dal riuso devono assicurarsi che l'accesso ai dati e il loro riutilizzo avvenga da remoto, all'interno di un ambiente di trattamento sicuro, fornito o controllato dall'ente pubblico, oppure all'interno dei locali fisici in cui si trova l'ambiente di trattamento sicuro, nel rispetto di rigorose norme di sicurezza, qualora l'accesso remoto non possa essere consentito senza compromettere i diritti e gli interessi di terzi[42].

La disciplina contempla anche l'ipotesi di *secondary use* dei dati in assenza di anonimizzazione e di una specifica base giuridica per la trasmissione dei dati personali a soggetti terzi (*data users*). In tal caso l'art. 5, par. 5, del DGA prevede che "l'ente pubblico si adoper[i] al meglio, conformemente al diritto dell'Unione e nazionale, per fornire assistenza ai potenziali riutilizzatori nel *richiedere il consenso degli interessati o l'autorizzazione dei titolari dei dati* i cui diritti e interessi possono essere interessati da tale riutilizzo, ove ciò sia fattibile senza un onere sproporzionato per l'ente pubblico (…)", con la precisazione che "qualora fornisca tale assistenza, l'ente pubblico può essere assistito dagli organismi competenti (…)".

Immaginando una difficoltà tecnica strutturale degli enti pubblici a svolgere le attività connesse al riuso dei dati appartenenti a categorie protette che sono nella loro disponibilità per i compiti istituzionali che già svolgono, la disciplina ha previsto, opportunamente, la facoltà di essere coadiuvati da organismi dotati delle necessarie competenze ad attuare le strategie di riuso degli enti, con costi che possono essere assorbiti e recuperati tramite un sistema di tariffazione volto a garantire la sostenibilità delle operazioni[43].

I predetti enti, infatti, in base all'art. 7 del DGA, possono farsi eventualmente assistere da "organismi competenti", dotati di risorse giuridiche, finanziarie, tecniche, umane e di know-how, aventi il compito di fornire assistenza tecnica agli anti pubblici impegnati nel riuso, finanche mettendo a loro disposizione un *ambiente di trattamento sicuro* per la fornitura dell'accesso, nonché sulle modalità per garantire tecnicamente, anche con tecniche di pseudonimizzazione, anonimizzazione,

41. In tal senso v. art. 5, par. 3, lett. *a)*, del DGA.

42. V. art. 5, par. 3, lett. *b)* e *c)*, del DGA.

43. Diversamente dalla disciplina sull'open data, con il *Data Governance Act* possono essere richieste delle tariffe da parte degli enti pubblici che mettano a disposizione i dati per il *secondary use* e ciò anche per coprire i costi necessari per porre in essere le attività di anonimizzazione o di raccolta del consenso degli interessati previste dalla disciplina in parola. L'art. 6, par. 1, del DGA, infatti, espressamente stabilisce che "Gli enti pubblici che consentono il riutilizzo delle categorie di dati di cui all'articolo 3, paragrafo 1, possono imporre tariffe per consentire

generalizzazione, soppressione, randomizzazione o altri metodi all'avanguardia, il rispetto dei requisiti e dei limiti previsti dalla disciplina sulla protezione dei dati personali, nonché per richiedere, se del caso, il consenso al riuso dei dati da parte degli interessati o dell'autorizzazione da parte dei titolari dei dati, e quant'altro si rendesse necessario per l'applicazione della disciplina in esame[44].

Il modello incentrato sul riuso dei dati detenuti dagli enti pubblici a beneficio anche della società civile e delle imprese può essere dunque interpretato, al di là delle etichette usate dal legislatore europeo nel *Data Governance Act*, come un modello di *data intermediation* in ambito pubblico.

L'intermediazione dei dati, a prescindere dal modello di riferimento, è pensata come uno strumento delineato per incentivare il *riuso* dei dati, esaltando quella *libera circolazione* delle informazioni, personali e non personali, che finora è risultata sottodimensionata, in quanto imbrigliata sia da vincoli normativi volti ad assicurare un rigido sistema di protezione dai rischi derivanti dal trattamento, sia da dinamiche di mercato chiuse, segnate da fenomeni di concentrazione in mano di pochi, desiderosi di sfruttare per sé il potenziale economico, e dunque non incentivati a consentirne la circolazione o alla condivisione in favore del concomitante interesse altrui o di quello collettivo.

4. Intermediazione dei dati nel nuovo scenario normativo avutosi con il Regolamento EHDS in tema di spazi di condivisione di dati sanitari

4.1. L'intermediazione in ambito pubblico dal *Data Governance Act* al Regolamento sull'*European Health Data Space*

A ben guardare il fenomeno del riuso dei dati detenuti da enti pubblici e da questi intermediati, in proprio o tramite altri "organismi competenti" che operano in ambienti sicuri di trattamento, è intimamente connesso a quello, di più recente introduzione, avutosi con la predisposizione degli spazi di condivisione dei dati, enunciato con enfasi nella Comunicazione della Commissione europea su *Una strategia europea per i dati* e poi regolamentato,

il riutilizzo di tali dati". Al contrario, la Direttiva 2019/1024/UE del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione nel settore pubblico prevede, all'art. 6 ("Principi di tariffazione"), par. 1, che "Il riutilizzo di documenti è gratuito", anche se poi il principio di gratuità è stemperato subito dopo dalla previsione di un'eccezione: "Tuttavia, può essere autorizzato il recupero dei costi marginali sostenuti per la riproduzione, messa a disposizione e divulgazione dei documenti, nonché per l'anonimizzazione di dati personali o per le misure adottate per proteggere le informazioni commerciali a carattere riservato (…)". Fanno altresì eccezione, ai sensi del par. 2, gli "enti pubblici che devono generare proventi per coprire una parte sostanziale dei costi inerenti allo svolgimento dei propri compiti di servizio pubblico", le "biblioteche, comprese le biblioteche universitarie, musei e archivi" e le "imprese pubbliche", ai quali non si applica il principio di gratuità per il riutilizzo.

44. Segnatamente, l'assistenza fornita dagli *organismi competenti* agli *enti pubblici* per il *riuso dei dati* appartenenti a categorie protette (incluso i dati personali) da questi detenuti, comprende, "ove necessario: a) fornire assistenza tecnica mettendo a disposizione un *ambiente di trattamento sicuro* per la fornitura dell'accesso ai fini del riutilizzo dei dati; b) fornire orientamenti e assistenza tecnica su come strutturare e conservare al meglio i dati per renderli facilmente accessibili; c) fornire assistenza tecnica per la *pseudonimizzazione* e garantire il trattamento dei dati in modo da tutelare efficacemente la vita privata, la riservatezza, l'integrità e l'accessibilità delle informazioni contenute nei dati per i quali è consentito il riutilizzo, comprese le tecniche di *anonimizzazione, generalizzazione, soppressione e randomizzazione* dei dati personali o altri metodi all'avanguardia di tutela della vita privata, e la *cancellazione* di informazioni commerciali riservate, tra cui segreti commerciali o contenuti protetti da diritti di proprietà intellettuale; d) se del caso, fornire assistenza agli enti pubblici affinché aiutino i riutilizzatori a *richiedere agli interessati il consenso al riutilizzo o ai titolari dei dati l'autorizzazione al riutilizzo*, in linea con le loro decisioni specifiche, anche in merito alla giurisdizione in cui si intende effettuare il trattamento dei dati, e fornire assistenza agli enti pubblici nell'istituire meccanismi tecnici che permettano di trasmettere le richieste di consenso o di autorizzazione formulate dai riutilizzatori, ove ciò sia fattibile nella pratica; e) fornire assistenza agli enti pubblici in merito alla valutazione dell'adeguatezza degli impegni contrattuali assunti da un riutilizzatore (…)" (v. art. 7, par. 4, DGA).

con riguardo ai dati sanitari, dal Regolamento EHDS (*European Health Data Space*).

Ne costituisce, in qualche modo, anche l'antecedente giuridico.

Si pensi al tenore del considerando n. 24 del *Data Governance Act*, nel quale si menziona il riutilizzo dei dati nel settore della sanità pubblica, con riguardo ai dati detenuti da soggetti operanti nel settore sanitario (come ad esempio di ospedali pubblici) e la creazione di ambienti di condivisione nell'Ue quali lo spazio europeo di dati sanitari, con obbligo di utilizzo di un ambiente di trattamento sicuro quale modalità tecnica per assicurare il rispetto della protezione delle persone fisiche, dei loro dati personali e della loro vita privata[45].

Sono temi che, anticipati nel Regolamento sulla governance europea dei dati, trovano una loro dettagliata attuazione nell'ambito del successivo Regolamento sullo spazio di condivisione dei dati sanitari. Infatti il Reg. EHDS, nella parte relativa al *secondary use* dei dati sanitari ospitati nello spazio di condivisione dei dati provenienti dalle strutture sanitarie, essenzialmente pubbliche, ripropone il medesimo modello di fondo, basato sull'intermediazione di dati personali svolta da enti pubblici, con l'assistenza di organismi competenti, in ambienti sicuri di trattamento, tracciato, in via embrionale e con caratteri generali, nel *Data Governance Act*.

Ritornano, tra i due modelli di intermediazione in ambito pubblico, con necessari riadattamenti ed evoluzioni, anche i principali istituti giuridici che hanno caratterizzato il fenomeno dell'intermediazione dei dati, tra cui, primariamente, il *diritto alla portabilità* dei dati e l'esercizio della *delega*.

4.2. 4.2. Il diritto alla portabilità dei dati nel Regolamento EHDS e il rapporto con il diritto alla *data portability* delineato nel GDPR

Quanto al diritto alla portabilità dei dati previsto nella nuova disciplina sugli spazi di condivisione dei dati, il considerando n. 23 del Reg. EHDS chiarisce il rapporto con il diritto alla portabilità di cui all'art. 20 del GDPR, rimarcandone la complementarità. Ivi si afferma, infatti, che il nuovo regolamento in tema di *European Health Data Space* "(…) stabilisce *diritti complementari* per le persone fisiche in merito all'uso primario, *che vanno al di là dei diritti di accesso e portabilità sanciti dal regolamento (UE) 2016/679 e li integrano* (…)".

Il diritto di cui all'art. 20 del GDPR, dunque, rimane fermo ed inalterato anche nella materia *de qua*, nella quale si aggiunge l'introduzione di una disciplina ulteriore, integrativa e complementare, del diritto alla portabilità per gli spazi di condivisione di dati sanitari, prevista all'art. 7 del

45. Nel considerando n. 24 del DGA, in particolare, viene affermato che "Al fine di creare fiducia nei meccanismi di riutilizzo, può essere necessario prevedere condizioni più rigorose per determinati tipi di dati non personali che possono essere ritenuti altamente sensibili in futuri specifici atti legislativi dell'Unione per quanto riguarda il trasferimento a paesi terzi, se tale trasferimento può compromettere obiettivi di politica pubblica dell'Unione, in linea con gli impegni internazionali. Nel *settore della sanità*, ad esempio, determinati set di *dati detenuti da soggetti operanti nel sistema sanitario pubblico*, quali gli *ospedali pubblici*, potrebbero essere considerati dati sanitari altamente sensibili. Altri settori pertinenti comprendono i trasporti, l'energia, l'ambiente e la finanza. Per garantire pratiche armonizzate in tutta l'Unione, tali tipologie di dati pubblici non personali altamente sensibili dovrebbero essere definite dal diritto dell'Unione, ad esempio nel contesto dello *spazio europeo dei dati sanitari* o di altra normativa settoriale. È opportuno stabilire mediante atti delegati tali condizioni cui è subordinato il trasferimento di tali dati a paesi terzi. Le condizioni dovrebbero essere proporzionate, non discriminatorie e necessarie per tutelare i legittimi obiettivi di politica pubblica dell'Unione individuati, quali la protezione della salute pubblica, la sicurezza, l'ambiente, la morale pubblica e la protezione dei consumatori, della vita privata e dei dati personali. Le condizioni dovrebbero corrispondere ai rischi identificati in relazione alla *sensibilità di tali dati, anche in termini di rischi di reidentificazione dei singoli individui*. Tali condizioni potrebbero includere termini applicabili per il trasferimento o modalità tecniche, quali l'*obbligo di utilizzare un ambiente di trattamento sicuro*, limiti relativi al riutilizzo dei dati nei paesi terzi o categorie di persone aventi facoltà di trasferire tali dati a paesi terzi o che possono accedere ai dati nel paese terzo. In casi eccezionali tali condizioni potrebbero inoltre comprendere restrizioni al trasferimento dei dati a paesi terzi per tutelare l'interesse pubblico".

Reg. EHDS, su cui le autorità di protezione dei dati personali continuano ad esercitare i propri poteri[46].

Le ragioni che hanno indotto ad una disciplina integrativa del diritto alla portabilità sono evidenti. Quello previsto, seppur innovativamente, all'art. 20 del GDPR soffre di evidenti limitazioni.

La prima concerne la base giuridica del trattamento, venendosi a configurare solamente qualora la condizione di liceità sia il consenso, *ex* art. 6, par. 1, lett. a), o art. 9, par. 2, lett. a), del GDPR, o il contratto, *ex* art. 6, par. 1, lett. b), GDPR. Ciò porterebbe ad escludere l'applicazione del diritto alla portabilità ove la base giuridica fosse di diverso tipo, come ben potrebbe avvenire per i trattamenti di dati sanitari svolti in ambito pubblico, tenendo conto, tra l'altro, che la natura particolare dei dati sanitari rende insufficiente ed inadeguato il ricorso alle condizioni di liceità contemplate all'art. 6 del GDPR.

La seconda limitazione riguarda la fonte dei dati, giacché il diritto alla portabilità previsto nella disciplina generale sulla protezione dei dati prevede la sua esercitabilità solamente con riguardo ai dati personali che siano stati "*forniti*" dall'interessato al titolare del trattamento, includendo dunque sia quelli espressamente ed attivamente conferiti dall'interessato, sia quelli raccolti dal titolare mediante l'osservazione di dati "grezzi" (*raw data*) [47], ma escludendo i dati che siano stati oggetto di successiva elaborazione da parte del titolare del trattamento o che siano stati da questi generati[48].

Una terza limitazione riscontrabile nel diritto alla portabilità dei dati di cui all'art. 20 GDPR si

46. Nel considerando n. 23 cit., infatti, il nuovo regolamento si preoccupa di rimarcare che "Le autorità di controllo istituite ai sensi del regolamento (UE) 2016/679 sono competenti per monitorare e assicurare l'applicazione di tale regolamento, in particolare per il monitoraggio del trattamento dei dati sanitari elettronici personali e per rispondere a eventuali reclami presentati dalle persone fisiche interessate (...)", aggiungendo altresì, con riguardo ai nuovi diritti complementari di accesso e di portabilità, che "(…) tali ulteriori diritti dovrebbero essere garantiti anche dalle autorità di controllo istituite a norma del regolamento (UE) 2016/679", ragion per cui "(…) gli Stati membri dovrebbero provvedere affinché le autorità di controllo siano dotate delle risorse umane e finanziarie, dei locali e delle infrastrutture necessari per l'efficace adempimento di tali compiti aggiuntivi (…)".

47. Article 29 Data Protection Working Party (WP29), *Guidelines on the right to data portability*, Revised and adopted on 5 April 2017, WP 242 rev.01, p. 9, ove si rimarca che "There are many examples of personal data, which will be knowingly and actively "provided by" the data subject such as account data (e.g. mailing address, user name, age) submitted via online forms. Nevertheless, data "provided by" the data subject also result from the observation of his activity. As a consequence, the WP29 considers that to give its full value to this new right, "provided by" should also include the personal data that are observed from the activities of users such as raw data processed by a smart meter or other types of connected objects, activity logs, history of website usage or search activities (…)".

48. WP29, Guidelines on the right to *data portability*, cit., p. 10, ove viene evidenziato che tra i dati forniti, oggetto di osservazione da parte del titolare del trattamento, non possono essere inclusi " (…) data that are created by the data controller (using the data observed or directly provided as input) such as a user profile created by analysis of the raw smart metering data collected". Sicché, "A distinction can be made between different categories of data, depending on their origin, to determine if they are covered by the right to *data portability*. The following categories can be qualified as 'provided by the data subject': – Data actively and knowingly provided by the data subject (for example, mailing address, user name, age, etc.). – Observed data provided by the data subject by virtue of the use of the service or the device. They may for example include a person's search history, traffic data and location data. It may also include other raw data such as the heartbeat tracked by a wearable device. In contrast, inferred data and derived data are created by the data controller on the basis of the data "provided by the data subject". For example, the outcome of an assessment regarding the health of a user or the profile created in the context of risk management and financial regulations (e.g. to assign a credit score or comply with anti-money laundering rules) cannot in themselves be considered as "provided by" the data subject. Even though such data may be part of a profile kept by a data controller and are inferred or derived from the analysis of data provided by the data subject (through his actions for example), these data will typically not be considered as "provided by the data subject" and thus will not be within scope of this new right. In general, given the policy objectives of the right to *data portability*, the term 'provided by the data subject' must be interpreted broadly, and should exclude 'inferred data' and 'derived data', which include personal data that are created by a service provider (for example, algorithmic results). A data controller can exclude those inferred data but should include

riscontra nella possibilità di ottenere il trasferimento dei dati da un titolare ad un altro solamente qualora l'operazione sia "tecnicamente fattibile"[49]. Ciò finisce per escludere l'esercizio del diritto alla portabilità dei dati nel caso in cui il titolare del trattamento riscontri (non una mera difficoltà ma una sostanziale) impossibilità tecnica nel realizzare la portabilità dei dati mediante la trasmissione diretta ad altro titolare del trattamento, in formato strutturato e leggibili da dispositivo. Ciò potrebbe avvenire, ad esempio, nei casi in cui non v'è a monte l'interoperabilità tra i dati o tra un sistema di trattamento e l'altro.

V'è poi una quarta limitazione, che si estrare dalla lettura di sistema nel combinato disposto con l'art. 12 del GDPR: di fronte alla richiesta di esercizio del diritto alla portabilità, come di qualsiasi altro diritto previsto nella disciplina generale in materia di protezione dei dati personali, il titolare del trattamento non ha l'obbligo di immediata esecuzione. Come previsto nel par. 3 della disposizione normativa da ultimo cit., "Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 [e dunque anche ai sensi dell'art. 20 in tema di portabilità dei dati, *n.d.a.*] senza ingiustificato ritardo e, comunque, al più tardi *entro un mese* dal ricevimento della richiesta stessa. Tale termine può essere *prorogato di due mesi*, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato"[50]. Anche il difetto di immediatezza del trasferimento, non certo ottimale in ambito sanitario soprattutto in relazione alle esigenze di cura dei pazienti, ha reso indispensabile l'emanazione di una disciplina *ad hoc* per gli spazi di condivisione di dati sanitari.

Si comprende bene, dunque, la ragione che ha portato all'avvento di un diritto alla portabilità, nell'art. 7 del Reg. EHDS, complementare ed integrativo rispetto all'analogo diritto alla portabilità previsto nell'art. 20 GDPR[51], che in un certo qual modo vede estendere la sua portata applicativa al nuovo contesto[52].

La correlazione è evidente, sia per la dichiarata competenza dell'autorità in materia di protezione dei dati personali anche su tali diritti di nuova (ri)formulazione, sia per il chiaro tenore del considerando n. 15 del Reg. EHDS, nel quale si ribadisce testualmente che "Il quadro stabilito dal presente regolamento dovrebbe basarsi sul diritto

all other personal data provided by the data subject through technical means provided by the controller. Thus, the term 'provided by' includes personal data that relate to the data subject activity or result from the observation of an individual's behaviour, but does not include data resulting from subsequent analysis of that behaviour".

49. In questo senso v. l'art. 20, par. 2, GDPR.

50. Art. 12, par. 3, GDPR. Inoltre, qualora si registri il caso di mancata ottemperanza "alla richiesta dell'interessato, il titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale" (art. 12, par. 4, GDPR).

51. La *ratio* è scolpita nel testo del considerando n. 14 del nuovo regolamento sugli spazi di condivisione dei dati sanitari, ove si legge che "Ai sensi del regolamento (UE) 2016/679 il diritto alla portabilità dei dati è limitato ai dati trattati sulla base del consenso o di un contratto e forniti dall'interessato a un titolare del trattamento. Inoltre, ai sensi dello stesso regolamento, le persone fisiche hanno il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro solo se tecnicamente fattibile. Tale regolamento non prevede tuttavia l'obbligo di rendere questa trasmissione diretta tecnicamente fattibile. Il diritto alla portabilità dei dati dovrebbe essere integrato nel quadro del presente regolamento, così da consentire alle persone fisiche di rendere accessibili almeno le categorie prioritarie dei loro dati sanitari elettronici personali ai professionisti sanitari di loro scelta, di scambiarli con questi e di scaricarli. Inoltre, alle persone fisiche dovrebbe essere garantito il diritto di chiedere a un prestatore di assistenza sanitaria la trasmissione di una parte dei loro dati sanitari elettronici a un destinatario chiaramente identificato nel settore della sicurezza sociale o dei servizi di rimborso. Tale trasmissione dovrebbe avvenire in una sola direzione".

52. Cfr. considerando n. 15 del Reg. EHDS.

alla portabilità dei dati previsto dal regolamento (UE) 2016/679 garantendo che le persone fisiche, in qualità di interessati, possano trasmettere i loro dati sanitari elettronici personali, compresi i dati desunti, nel formato europeo di scambio delle cartelle cliniche elettroniche, a prescindere dalla base giuridica per il trattamento dei dati sanitari elettronici. I professionisti sanitari dovrebbero astenersi dall'ostacolare l'applicazione dei diritti delle persone fisiche, ad esempio rifiutandosi di tenere conto dei dati sanitari elettronici personali provenienti da un altro Stato membro e forniti tramite il formato europeo di scambio delle cartelle cliniche elettroniche, interoperabile e affidabile".

In tale contesto, la disciplina del "Diritto delle persone fisiche alla portabilità dei dati" è scolpita nell'art. 7 del nuovo regolamento, nel quale viene stabilito, nel par. 1, che "Le persone fisiche hanno il diritto di *concedere l'accesso* alla totalità o a parte dei loro dati sanitari elettronici personali *a un altro prestatore* di assistenza sanitaria di loro scelta *o di chiedere a un prestatore di assistenza sanitaria di trasmettere* la totalità o parte dei loro dati sanitari elettronici a un altro prestatore di assistenza sanitaria di loro scelta *immediatamente*, gratuitamente e senza ostacoli da parte del prestatore di assistenza sanitaria o dei fabbricanti dei sistemi utilizzati dal prestatore di assistenza sanitaria"[53].

Si noti che nell'art. 20 GDPR la *data portability* trova esecuzione nelle forme del trasferimento dei dati, in formato strutturato e leggibile da dispositivo elettronico (i) all'interessato medesimo (che, dunque, riceve i dati personali con facoltà di ritrasmetterli ad altro titolare senza che il primo possa ostacolare tale trasferimento), oppure (ii) direttamente verso altro titolare del trattamento, ove ciò risulti tecnicamente fattibile (nella declinazione della *data portability* del diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro). Nell'art. 7 del nuovo regolamento, invece, le modalità esecutiva – e dunque i contenuti stessi del diritto – appaiono diversi, in quanto il sistema di trattamento rimane il medesimo, quello assicurato dallo spazio di condivisione dei dati, e il diritto a ricevere e trasmettere o a veder trasferiti da un soggetto ad un altro i propri dati personali entro i tempi (dilatati) congrui all'esecuzione della prestazione richiesta e non preventivata, assume, *in primis*, la diversa fisionomia del diritto a far ottenere (e dunque a *concedere*) un *accesso condiviso* a tutti o a parte dei propri dati e, *in secundis*, il diritto all'*immediata trasmissione* dei dati tra un prestatore di assistenza sanitaria ed un altro, ossia non tra un qualsiasi titolare del trattamento ed un qualsiasi altri titolare del trattamento, ma tra titolari qualificati in ragione della specifica natura dell'attività da questi svolta[54].

V'è poi la portabilità dei dati che si esercita, ai sensi dell'art. 7 , par. 4, del Reg. cit., scaricando, da parte delle persone fisiche, "*una copia elettronica delle loro categorie prioritarie di dati sanitari elettronici personali* in conformità dell'articolo 3, paragrafo 2" per poi "*trasmettere tali dati ai prestatori di assistenza sanitaria di loro scelta* nel formato europeo di scambio delle cartelle cliniche elettroniche di cui all'articolo 15" e, in tal caso, "*Il prestatore di assistenza sanitaria ricevente deve accettare tali dati* e, se del caso, essere in grado di leggerli".

Si tratta tuttavia di una portabilità funzionale alla realizzazione del sistema di trattamento protetto, che avviene entro il "recinto" sicuro degli spazi di condivisione dei dati, amministrati centralmente e svolto solamente verso soggetti predeterminati: appunto, i "prestatori di assistenza sanitaria" o i "destinatari chiaramente identificati del settore della sicurezza sociale o dei servizi di

53. Al par. 2 di tale articolo di prevede poi che "Qualora i prestatori di assistenza sanitaria si trovino in Stati membri diversi, le persone fisiche hanno il diritto di chiedere la trasmissione dei loro dati sanitari elettronici personali nel formato europeo di scambio delle cartelle cliniche elettroniche di cui all'articolo 15 attraverso l'infrastruttura transfrontaliera di cui all'articolo 23. Il prestatore di assistenza sanitaria ricevente deve accettare tali dati ed è in grado di leggerli".

54. Ciò anche qualora, ai sensi del par. 3 del medesimo articolo, le persone fisiche esercitino il diritto loro riconosciuto alla portabilità dei dati quale "diritto di *chiedere* a un prestatore di assistenza sanitaria *di trasmettere* una parte dei loro dati sanitari elettronici personali a un *destinatario chiaramente identificato del settore della sicurezza sociale o dei servizi di rimborso* (…)", con l'ulteriore precisazione che "Tale trasmissione avviene *immediatamente*, gratuitamente e senza ostacoli da parte del prestatore di assistenza sanitaria o dei fabbricanti dei sistemi utilizzati dal prestatore di assistenza sanitaria *ed è solo unidirezionale*".

rimborso". Non è, questa, una portabilità pensata per i fornitori dei servizi di intermediazione di dati di cui al *Data Governance Act*. È, dunque, una portabilità "tipizzata", preordinata al trasferimento dei dati a figure soggettive predeterminate, incentrata sull'*uso primario* dei dati, come attesta anche la collocazione dell'art. 7 del Reg. EHDS nell'ambito della Sez. II ("Diritti delle persone fisiche in relazione all'*uso primario* dei loro dati sanitari elettronici personali e relative disposizioni") del Capo II (intitolato proprio all'"Uso primario")[55].

Poiché tuttavia i dati presenti nello spazio di condivisione dei dati vengono poi destinati, obbligatoriamente, anche all'uso secondario, in base alla disciplina delineata nel Capo IV ("Uso secondario") del Reg. EHDS, agli artt. 50 ss.[56], risulta evidente che chi gestisce lo spazio di condivisione dei dati finisce per assumere sostanzialmente il ruolo di *intermediario* istituzionalizzato, con un apparato normativo che ottimizza, per il settore sanitario, l'esperienza normativa già maturata nel settore dell'intermediazione dei dati con il *Data Governance Act*. Il riferimento è, in particolare, al ruolo di intermediazione sostanzialmente svolto dagli enti pubblici, con riguardo ai dati da questi detenuti per fini istituzionali, che possono essere forniti agli "utenti di dati" mediante il ricorso ad "organismi competenti", con applicazione di un sistema tariffario che permetta la sostenibilità del servizio.

Si tratta ovviamente di un'innovazione importante ed apprezzabile, destinata ad un significativo potenziamento, per le finalità indicate nell'art. 53 del Reg EHDS, anche in ragione della ricerca di settore, nonché dello sviluppo e dell'innovazione

55. La definizione di "uso primario" è esplicitata all'art. 2, par. 2, lett. d), del Reg. EHDS, ai sensi del quale tale sintagma viene inteso come "il trattamento dei dati sanitari elettronici per la prestazione di assistenza sanitaria al fine di valutare, mantenere o ripristinare lo stato di salute della persona fisica cui si riferiscono tali dati, comprese la prescrizione, la dispensazione e la fornitura di medicinali e dispositivi medici, nonché per i pertinenti servizi sociali, amministrativi o di rimborso".

56. Si consideri che all'art. 51 del Reg. EHDS vengono indicate le categorie minime che sono soggette all'obbligo di disponibilità per l'uso secondario, posto in essere a carico dei titolari dei trattamenti di dati sanitari che ne sono già in possesso per l'uso primario, con facoltà accordata agli Stati membri di inserire categorie di dati aggiuntive. Ai sensi dell'art. 51 dianzi citato, infatti, "I *titolari dei dati sanitari mettono a disposizione per l'uso secondario*, conformemente al presente capo, le categorie di dati sanitari elettronici seguenti: a) dati sanitari elettronici provenienti da cartelle cliniche elettroniche; b) dati su fattori con un'incidenza sulla salute, compresi i determinanti socioeconomici, ambientali e comportamentali della salute; c) dati aggregati sulle esigenze di assistenza sanitaria, sulle risorse assegnate all'assistenza sanitaria, sulla prestazione di assistenza sanitaria e sul suo accesso, sulla spesa per l'assistenza sanitaria e sul suo finanziamento; d) dati sugli agenti patogeni che incidono sulla salute umana; e) dati amministrativi relativi all'assistenza sanitaria, anche relativamente alle dispensazioni, alle domande di rimborso e ai rimborsi; f) dati genetici, epigenomici e genomici umani; g) altri dati molecolari umani, quali quelli provenienti dalla proteomica, dalla trascrittomica, dalla metabolomica, dalla lipidomica e altri dati omici; h) dati sanitari elettronici personali generati automaticamente mediante dispositivi medici; i) dati provenienti dalle applicazioni per il benessere; j) dati relativi allo status e alla specializzazione e all'istituzione dei professionisti sanitari coinvolti nella cura di una persona fisica; k) dati provenienti da registri dei dati sanitari basati sulla popolazione, come i registri di sanità pubblica; l) dati provenienti da registri medici e da registri della mortalità; m) dati provenienti da sperimentazioni cliniche, studi clinici, indagini cliniche e studi delle prestazioni soggetti al regolamento (UE) n. 536/2014, al regolamento (UE) 2024/1938 del Parlamento europeo e del Consiglio (35), al regolamento (UE) 2017/745 e al regolamento (UE) 2017/746; n) altri dati sanitari provenienti da dispositivi medici; o) dati provenienti da registri di medicinali e dispositivi medici; p) dati provenienti da coorti di ricerca, questionari e indagini in materia di salute, dopo la prima pubblicazione dei risultati; q) dati sanitari provenienti da biobanche e banche dati associate". Così il comma 1, a cui segue poi, al comma 2, l'ulteriore possibile estensione di tali categorie minime da conferire obbligatoriamente per l'uso secondario dei dati, rimesse alle scelte degli ordinamenti nazionali: "Gli Stati membri possono stabilire nel loro diritto nazionale che categorie *aggiuntive* di dati sanitari elettronici siano messe a disposizione per l'uso secondario in conformità del presente regolamento".

di prodotti e servizi e per l'addestramento dei sistemi di intelligenza artificiale[57].

L'accesso ai dati di uso secondario è riservato a enti pubblici e a istituzioni, organi e organismi dell'Ue solamente per alcune delle finalità ammesse, desumendosi quindi un'apertura anche ai soggetti privati per le finalità, anche di ricerca scientifica in ambito sanitario e per le finalità ad essa strumentale, di innovazione di prodotti e servizi e per l'addestramento dei sistemi di IA[58].

4.3. L'istituto della delega nel Regolamento EHDS e servizi di *data intermediation*

Altro istituto rilevante nel fenomeno di intermediazione di dati, riscontrabile anche nella disciplina del Reg. EHDS, è quello della "delega", usato dai fornitori dei servizi di *data intermediation* per recuperare i dati dei propri utenti dai diversi titolari del trattamento e, una volta acquisiti, attuare per loro conto le strategie di *secondary use*.

Nel nuovo regolamento europeo sui dati personali la delega viene espressamente contemplata nel considerando n. 21, nel quale si trova affermato che "Le persone fisiche dovrebbero poter fornire un'*autorizzazione ad altre persone fisiche di loro scelta*, come a parenti o ad altre persone fisiche loro vicine, *che permetta a queste persone* di loro scelta *di accedere ai dati sanitari elettronici personali* delle persone fisiche che forniscono l'autorizzazione o *di controllarne l'accesso*, oppure *di utilizzare servizi di sanità digitale per loro conto*. Tali autorizzazioni potrebbero *anche risultare utili per altri usi* alle persone fisiche che ricevono l'autorizzazione. Per consentire e attuare tali autorizzazioni è opportuno che gli Stati membri istituiscano *servizi di delega* che dovrebbero essere collegati a servizi di accesso ai dati sanitari elettronici personali, quali portali per i pazienti o applicazioni per dispositivi mobili rivolte ai pazienti. I *servizi di delega* dovrebbero anche permettere ai tutori di agire per conto dei loro tutelati, compresi i minori; in tali situazioni le autorizzazioni potrebbero essere automatiche (…)".

Si tratta di strumento autorizzatorio con il quale l'interessato, in forza degli atti di autonomia

57. Nel cit. art. 53 del Reg. EHDS, rubricato "Finalità per le quali è possibile trattare i dati sanitari elettronici per l'uso secondario", si stabilisce, al par. 1, che "Gli organismi responsabili dell'accesso ai dati sanitari concedono l'accesso ai dati sanitari elettronici di cui all'articolo 51 per l'uso secondario a un utente dei dati sanitari solo se il trattamento dei dati da parte dell'utente è necessario per una delle finalità seguenti: a) pubblico interesse nell'ambito della sanità pubblica o della medicina del lavoro, come nel caso delle attività per la protezione da gravi minacce per la salute a carattere transfrontaliero, della sorveglianza della sanità pubblica o delle attività per la garanzia di elevati livelli di qualità e sicurezza dell'assistenza sanitaria, inclusa la sicurezza dei pazienti, e di medicinali o dispositivi medici; b) definizione delle politiche e attività regolamentari a sostegno di enti pubblici o di istituzioni, organi e organismi dell'Unione, comprese le autorità di regolamentazione, del settore sanitario o dell'assistenza affinché svolgano i compiti definiti nei rispettivi mandati; c) statistiche quali definite all'articolo 3, punto 1), del regolamento (UE) n. 223/2009, come le statistiche ufficiali a livello nazionale, multinazionale e dell'Unione, relative al settore sanitario o dell'assistenza; d) attività d'istruzione o d'insegnamento nel settore sanitario o dell'assistenza al livello della formazione professionale o dell'istruzione superiore; e) ricerca scientifica nel settore sanitario o dell'assistenza che contribuisce alla sanità pubblica o alla valutazione delle tecnologie sanitarie o che garantisce elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici, con l'obiettivo di favorire gli utenti finali, quali i pazienti, i professionisti sanitari e gli amministratori sanitari, tra cui: i) attività di sviluppo e innovazione per prodotti o servizi; ii) attività di addestramento, prova e valutazione degli algoritmi, anche nell'ambito di dispositivi medici, dispositivi medico-diagnostici in vitro, sistemi di IA e applicazioni di sanità digitale; f) miglioramento della prestazione di assistenza, ottimizzazione delle cure ed erogazione di assistenza sanitaria sulla base dei dati sanitari elettronici di altre persone fisiche".

58. Viene infatti previsto, all'art. 53, par. 2, del Reg. EHDS, che "L'accesso ai dati sanitari elettronici per le finalità di cui al paragrafo 1, lettere a), b) e c), è riservato agli enti pubblici e alle istituzioni, agli organi e agli organismi dell'Unione che esercitano i compiti loro affidati dal diritto dell'Unione o dal diritto nazionale, anche quando il trattamento dei dati per lo svolgimento di tali compiti è effettuato da terzi per conto di tali enti pubblici o delle istituzioni, degli organi e degli organismi dell'Unione". La riserva di accesso non si estende dunque alle finalità di cui alle lett. d), e) ed f), per le quali v. nt. precedente.

privata e di autodeterminazione informativa, per la cura dei propri interessi, conferisce ad un altro soggetto il potere di compiere atti o esercitare diritti per suo conto. In questo senso, la "delega" quale atto unilaterale autorizzatorio con cui si investe altri di poteri rappresentativi è accostabile alla "procura"[59]. Il considerando citato, come s'è avuto modo di evidenziare, prevede che la "delega" – cioè, in questo contesto, l'attribuzione del potere rappresentativo per l'esercizio del diritto da parte di un altro soggetto per il soddisfacimento di interessi del delegante – sia effettuata in favore di un'altra *persona fisica*, ipotizzando espressamente che ciò avvenga nei confronti di "parenti" o "altre persone fisiche loro vicine". Si tratta ovviamente di menzione del tutto esemplificativa, ma è pacifico che l'assenza di parentela o di vicinanza non siano ostative al conferimento della delega, purché vi sia comunque la fiducia dell'interessato nei confronti del soggetto delegato. Si tratta, infatti, di atto *intuitus personae*, che, com'è noto, non richiede affettività o vicinanza amicale o sentimentale, ma l'esistenza di un rapporto basato sulla valutazione positiva delle altrui caratteristiche personali del soggetto a cui ci si affida, sia egli persona fisica o giuridica[60]. Si consideri che, nel caso specifico degli spazi di

59. La dottrina definisce la "procura" come "un atto unilaterale, con il quale un soggetto investe un altro soggetto del potere di rappresentarlo; ed è un atto unilaterale recettizio nei confronti dei rappresentante, non recettizio nei confronti dei terzi: sotto questo aspetto non può dirsi rivolto ad un destinatario determinato, ma a tutti coloro con i quali il rappresentante si troverà a contrattare in nome del rappresentato". Così Galgano 2014. Per la delega in ambito amministrativo si rimanda, invece, a Miele 1962.

60. L'*intuitus personae* non esige, secondo la ricostruzione della dottrina dominante, che la relazione giuridica per il compimento dell'atto sia instaurata nei confronti di una persona fisica, potendo l'*intuitus personae* essere riferito anche nei riguardi delle persone giuridiche. Si pensi, ad esempio, alla disciplina del contratto di appalto, ove, dal divieto di subappalto – in assenza di espressa autorizzazione dal committente – si argomenta del connotato *intuitus personae* del contratto concluso dall'appaltatore, anche se questi non svolge la prestazione in prevalenza con il proprio lavoro personale. In questo senso cfr. Musolino 2011, il quale, sulla *ratio* del divieto di subappalto e l'*intuitus personae*, sostiene che "Secondo un orientamento, fine della statuizione *ex* art. 1656 c.c. sul divieto di subappalto sarebbe di evitare che l'imprenditore si trasformi in un accaparratore di lavori per scopi puramente speculativi. Tale posizione non appare, però, pienamente condivisibile, poiché comporterebbe l'indisponibilità della norma, in quanto sostanzialmente dettata per motivi di ordine pubblico. In realtà, il legislatore considera lecito il subappalto, qualora sia autorizzato dal committente, non perché affidi a quest'ultimo il compito di valutare quell'interesse pubblico, ma perché solo il suo interesse privato sta a fondamento del divieto, che quindi non ha più ragione di essere nel caso in cui l'interesse medesimo sia salvo. Si tratta dell'interesse del committente a che l'esecuzione dell'opera non venga effettuata da un'impresa senza che questa sia stata prima da lui autorizzata, poiché si è detto, anche in questa fattispecie, rilievo all'*intuitus personae*". Vero è che nell'appalto, diversamente dal contratto d'opera, non rileva che la prestazione sia eseguita personalmente dall'imprenditore, "tuttavia non si può ammettere, senza una specifica autorizzazione che l'appaltatore si liberi pure del compito di organizzazione, di direzione e di gestione, riversandolo sui subappaltatori" (*Ibidem*, p. 31). L'A. cit. aggiunge, *ivi* nella nt. 14, che "La considerazione secondo cui l'appalto è ascrivibile ai contratti stipulati intuitu personae è condivisa dalla dottrina dominate". Di diverso avviso è chi ha rilevato che "il c.d. *intuitus personae* negli appalti costituisce una sorta di retaggio di un'epoca nella quale l'esecuzione del contratto veniva affidata alle capacità – si potrebbe dire – personali dell'imprenditore/appaltatore. Ovviamente una siffatta configurazione è assai lontana dalla nostra realtà nella quale si è ormai in presenza di una dimensione aziendale che comporta inevitabilmente la "spersonalizzazione" del contratto di appalto. Anzi, l'*intuitus* personale – quantomeno nella contrattazione pubblica – sembra mutare di significato: infatti, mentre nell'accezione tradizionale esso implicava l'impossibilità di trasferire ad altro soggetto l'esecuzione del contratto, oggigiorno pare emergere un'esigenza di immodificabilità del contraente riferita, tuttavia, non più alla figura di un determinato imprenditore, bensì a un determinato complesso aziendale". Così Alberti 2008. Si veda anche la lettura critica, quanto all'*intuitus personae* nei contratti di appalto, enunciata da Iudica 2009. Sulla pacifica riferibilità dei contratti *intuitus personae* anche alle persone giuridiche si veda anche Galgano 2014, p. 405, nota n. 70, il quale esemplificativamente fa riferimento a "quanto l'art. 1918, commi 3° e 4°, prevede per il caso di alienazione della cosa assicurata:

condivisione di dati sanitari, le ragioni che inducono a delegare un altro soggetto potrebbero essere diverse, incluso il difetto di competenze tecnologiche, come potrebbe capitare ad esempio con le persone anziane che non abbiano dimestichezza con la complessità della soluzione tecnologica proposta con l'EHDS[61].

Nel testo normativo il tema è disciplinato all'art. 4 del Regolamento, rubricato "Servizi di accesso ai dati sanitari elettronici per le persone fisiche e i loro rappresentanti", nel quale, dopo aver menzionato, al par. 1, l'istituzione di "uno o più servizi di accesso ai dati sanitari elettronici a livello nazionale, regionale o locale" per consentire in tal modo "alle persone fisiche di accedere ai loro dati sanitari elettronici personali e di esercitare i loro diritti di cui all'articolo 3 e agli articoli da 5 a 10", viene ulteriormente precisato che "tali servizi di accesso sono gratuiti per le persone fisiche e i loro rappresentanti di cui al paragrafo 2 del presente articolo".

Qui entra in gioco il meccanismo della "delega", di cui si prevede l'istituzione in forma di "servizio", quale "funzionalità di servizio di accesso ai dati sanitari elettronici", in favore sia dei "rappresentati legali delle persone fisiche", sia delle persone fisiche scelte dagli interessati e da questi autorizzati, tramite il sistema di gestione delle autorizzazioni, "ad accedere ai loro dati sanitari elettronici personali, o anche a una parte di essi, per un periodo determinato o indeterminato e, in caso di necessità, solo per una finalità specifica"[62].

Si noti che il termine *delega* è usato impropriamente con riguardo ai "rappresentanti legali delle persone fisiche", in quanto allude, generalmente, all'attribuzione volontaria del potere rappresentativo, mentre la rappresentanza legale ha la sua fonte nella legge e non nell'atto di autonomia privata.

V'è però da rilevare che il meccanismo di delega è comunque strutturato nell'ambito di un "servizio" fornito negli spazi di condivisione di dati sanitari, il che allude non solo all'atto autorizzatorio del delegare, ma anche all'allestimento tecnico del sistema informatico, tale da consentire, sia nella rappresentanza volontaria, sia in quella legale, di sostituire un soggetto (l'interessato) con un altro (il rappresentante designato in forza dell'atto di autonomia provata o quello individuato *ex lege*, come i genitori del minore o il tutore dell'incapace), abilitando quest'ultimo, dal punto di vista informatico, ad intervenire con le proprie credenziali sul sistema, svolgendo l'attività per conto dell'interessato medesimo[63], con un sistema interoperabile a

l'acquirente subentra nel contratto di assicurazione, ma l'assicuratore può recedere dal contratto; ed è quanto prevede, per i contratti relativi all'azienda ceduta, l'art. 2558, comma 2°: l'*intuitus personae* opera qui come 'giusta causa' di recesso del terzo contraente". Galgano traccia una linea di distinzione tra "contratti personali" e quelli "c.d. *intuitus personae*", che si hanno quando l'identità o le qualità personali di uno dei contraenti sono determinanti del consenso dell'altro o degli altri contraenti, anche qualora il contraente medesimo, di cui rilevano l'identità o le qualità personali, sia una persona giuridica.

61. Izzo-Guarda 2010.

62. Cfr. art. 4, par. 2, del Reg. EHDS, ove, testualmente, viene stabilito che "2. Gli Stati membri provvedono affinché siano istituiti uno o più *servizi di delega come funzionalità dei servizi di accesso* ai dati sanitari elettronici che consentano: a) alle persone fisiche di autorizzare altre persone fisiche di loro scelta ad accedere per loro conto ai loro dati sanitari elettronici personali, o a una parte di essi, per un periodo determinato o indeterminato e, in caso di necessità, solo per una finalità specifica, e di gestire tali autorizzazioni; e b) ai rappresentanti legali delle persone fisiche di accedere ai dati sanitari elettronici personali delle persone fisiche di cui curano gli interessi, conformemente al diritto nazionale. Gli Stati membri stabiliscono norme relative alle autorizzazioni di cui alla lettera a) del primo comma e alle azioni dei tutori e di altri rappresentanti legali".

63. La previsione del servizio di delega previsto nel Reg. EHDS, quale servizio tecnico-informatico in grado di abilitare il rappresentante (istituito *ex lege* o in base all'autonomia privata) ad agire per conto dell'interessato si ricollega, in un certo senso, alla previsione contenuta nell'art. 8, par. 2, GDPR, ove prevede che "Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili". Ciò che nel GDPR è rimesso all'*accountability* del titolare del trattamento, nel Reg. EHDS è istituzionalizzato con scelte predeterminate *ex lege*, rimesse agli Stati membri ai sensi dell'art. 4, par. 2, cit. ("Gli Stati membri provvedono affinché siano istituiti uno o più servizi di delega come funzionalità dei servizi di accesso ai dati sanitari elettronici…").

livello europeo che va adeguato alla disciplina del Regolamento eIDAS[64].

Del resto, ove non vi fosse il meccanismo tecnico del "servizio di delega", potrebbe verificarsi che di fatto l'interessato finisca materialmente per far utilizzare le proprie credenziali ad altri, nell'intento di far consentire comunque l'accesso al sistema di trattamento dei dati da parte di chi è chiamato ad agire per conto dell'interessato, quale rappresentante su base volontaria o per disposizione di legge[65].

Ciò che tuttavia risulta più difficilmente comprensibile, sul piano teorico-giuridico e sistematico, è la scelta di rendere delegabile l'accesso solamente nei confronti delle persone fisiche e non anche delle persone giuridiche.

Si tratta di opzione normativa che il legislatore italiano aveva già percorso con l'art. 9, co. 2, del d.lgs. 196/2023, prima dell'abrogazione ad opera del d.lgs. 101/2018, ove, con riguardo alle modalità di esercizio dei diritti dell'interessato, si prevedeva testualmente che "(…) l'interessato può conferire, per iscritto, delega o procura a persone fisiche, *enti*, *associazioni* od organismi (…)"[66] e "(…) può, altresì, farsi assistere da una persona di fiducia"[67]. Con la revisione del Codice in materia di protezione dei dati personali dovuta ad esigenze di coordinamento con il GDPR, l'art. 9 cit. è stato abrogato, senza però che fosse vietata la delega all'esercizio dei diritti dell'interessato, sulla base dei principi generali di diritto privato, che consente ad ogni persona dotata di capacità di agire di autorizzare altri al compimento di atti giuridici, quando ciò è in linea con il proprio interesse e purché non si tratti di atti personalissimi. Che l'esercizio dei diritti dell'interessato non sia atto personalissimo risulta evidente dall'art. 8 GDPR, che istituisce quali rappresentanti *ex lege*, per il consenso dei minori (ed ovviamente anche per l'esercizio dei diritti riconosciuti all'interessato), coloro che esercitano la responsabilità genitoriale, al di fuori dei casi in cui ai minori sia consentito agire personalmente nei limiti oggettivi e d'età previsti dal GDPR e dal Codice in materia di protezione dei dati personali[68].

64. In tal senso è significativa la parte finale del considerando n. 21 del Reg. EHDS, ove viene rimarcato che "I *servizi di accesso ai dati sanitari elettronici personali*, quali *portali per i pazienti o applicazioni per dispositivi mobili rivolte ai* pazienti, dovrebbero utilizzare tali autorizzazioni e consentire così alle persone fisiche autorizzate di accedere ai dati sanitari elettronici personali che rientrano nell'ambito dell'autorizzazione. Al fine di garantire una soluzione orizzontale con una maggiore facilità d'uso, *le soluzioni digitali per i servizi di delega dovrebbero essere in linea con il regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio e alle specifiche tecniche del portafoglio europeo di identità digitale*. Ciò contribuirebbe a ridurre gli oneri amministrativi e finanziari per gli Stati membri, riducendo il rischio di sviluppare sistemi paralleli non interoperabili a livello dell'Unione".

65. Il tema è stato trattato, con riguardo al FSE, e con riferimento all'impianto normativo precedente al GDPR, da Izzo-Guarda 2010, p. 25 s. Gli autori precisano efficacemente che "Come sempre accade nel caso di scelte regolative che attengono a scenari ove la volontà giuridicamente rilevante di un soggetto e i suoi effetti concreti sono mediati dal bit, una soluzione estrema che accarezzi l'idea di dire semplicemente no alla possibilità che l'interessato deleghi ad un altro soggetto la gestione del proprio interesse ai dati inerenti la propria salute innescherebbe il rischio assai concreto che le credenziali di accesso dell'interessato al sistema di sanità elettronica finiscano per essere comunque irritualmente rese".

66. Art. 9, par. 2, d.lgs. 196/2003 (corsivo aggiunto), prima della riforma avvenuta con il d.lgs. 101/2018, che ne ha comportato l'abrogazione formale.

67. *Ibidem*. Anche nella normativa precedente il principio era pacificamente affermato nel nostro ordinamento all'art. 13, co. 4, della l. n. 675/1996, poi confluito con modifiche nel Codice in materia di protezione dei dati personali (d.lgs. n. 196/2023), ove si prevedeva la possibilità di delega o procura in forma scritta non solo a persone fisiche ma anche ad "associazioni" ("Nell'esercizio dei diritti di cui al comma 1 *l'interessato può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni*").

68. Com'è noto, l'art. 8, par. 1, GDPR prevede che "Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della

La scelta del Regolamento EHDS è stata quella di limitare la delega alle sole persone fisiche: nulla vieta tuttavia di individuare come destinatario della delega il legale rappresentante di una persona giuridica o un soggetto che operi all'interno di un ente, che si individua quale soggetto a cui ci si affida per la cura dell'interesse da salvaguardare. Del resto, qualora si individuasse come destinatario dell'autorizzazione una persona giuridica, in linea con quanto era contemplato dal testo originario dell'art. 9 del d.lgs. 196/2003, occorreva pur sempre individuare un soggetto, persona fisica, che agisse nell'ambito dell'ente e, in difetto di diversa precisazione, si sarebbe dovuto individuare nel legale rappresentante *pro-tempore*.

Ulteriori considerazioni vanno declinate con riguardo al particolare contesto in cui si colloca l'EHDS, quantomeno con riguardo all'uso primario dei dati sanitari personali, giacché ci si muove nell'ambito di quella che può essere definita una "*relazione di cura*" tra medico e paziente, in cui il trattamento dei dati personali è funzionale alla cura dell'interessato e all'assistenza sanitaria nei suoi confronti. Sicché va tenuto conto, in prospettiva sistematica, che nel nostro ordinamento entra in rilievo l'impianto delineato nella legge 22 dicembre 2017, n. 219 recante "Norme in materia di consenso informato e disposizioni anticipate di trattamento", nella parte in cui, all'art. 1, co. 2, vengono individuati nei *familiari*, nella *parte dell'unione civile*, nel *convivente* o in un'*altra persona di fiducia del paziente* i soggetti coinvolgibili, a discrezione del paziente medesimo, nella relazione di cura che si instaura tra paziente e medico[69], e, al successivo co. 3, viene previsto che il paziente possa indicare i familiari o altra persona di sua fiducia sia per ricevere, in sua vece, le informazioni sulle condizioni di salute del paziente (anche con riguardo alla diagnosi, alla prognosi, ai benefici e ai rischi degli accertamenti diagnostici e dei trattamenti sanitari, nonché alle possibili alternative e alle conseguenze dell'eventuale rifiuto del trattamento sanitario, dell'accertamento diagnostico o della rinuncia ai medesimi), sia per esprimere il consenso al trattamento sanitario, con annotazione nella cartella clinica e nel fascicolo sanitario elettronico[70].

responsabilità genitoriale. Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni". Lo Stato italiano, con l'art. 2-*quinquies* del novellato Codice in materia di protezione dei dati personali, ha determinato la soglia d'età a quattordici anni, precisando che "In attuazione dell'articolo 8, paragrafo 1, del Regolamento, il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale". Dunque, chi esercita la responsabilità genitoriale esprime per conto del minore il consenso – ed esercita i diritti dell'interessato – nei seguenti casi: a) qualora non trovi applicazione l'art. 6, par. 1, lett. a), ma l'art. 9, par. 1, l'art. a), GDPR – e dunque quando il trattamento nei cui confronti si esprime il consenso abbia ad oggetto dati particolari – a prescindere dalle soglie d'età e dalla natura di servizio della società dell'informazione offerto al minore; b) ove il trattamento nei cui confronti si chiede di esprimere il consenso non abbia ad oggetto i servizi della società dell'informazione offerti ai minori; c) qualora il minore non abbia ancora raggiunto i quattordici anni e il trattamento abbia ad oggetto servizi della società dell'informazione offerti ai minori e il consenso sia fondato sull'art. 6, par. 1, lett. *a)*, GDPR. Va poi precisato che, in tutti i casi in cui il trattamento riguardi minori e non sia fondato sul consenso, ma su altra base giuridica, chi esercita la responsabilità genitoriale potrà comunque esercitare per conto del minore tutti i diritti che sono riconosciuti all'interessato, quali rappresentati legali.

69. Testualmente, l'art. 1, co. 2, della l. n. 219/2017, prevede che "È promossa e valorizzata la relazione di cura e di fiducia tra paziente e medico che si basa sul consenso informato nel quale si incontrano l'autonomia decisionale del paziente e la competenza, l'autonomia professionale e la responsabilità del medico. Contribuiscono alla relazione di cura, in base alle rispettive competenze, gli esercenti una professione sanitaria che compongono l'equipe sanitaria. In tale relazione sono coinvolti, se il paziente lo desidera, anche i suoi familiari o la parte dell'unione civile o il convivente ovvero una persona di fiducia del paziente medesimo".

70. L'art. 1, co. 3, della l. n. 219/2017 stabilisce espressamente che "*Ogni persona ha il diritto di conoscere le proprie condizioni di salute e di essere informata in modo completo, aggiornato* e a lei comprensibile riguardo alla

Il "servizio di delega" previsto nel Regolamento EHDS, dunque, è ritagliato su questo modello, che si estende anche con riguardo al tema del trattamento dei dati personali di carattere sanitario, ben al di là dei confini del solo trattamento sanitario[71].

La questione della delega si incrocia con i modelli di intermediazione di dati in forma cooperativa recentemente disciplinati dal *Data Governance Act*[72], che trovano applicazione anche al settore sanitario[73].

Quando il testo di tale Regolamento europeo era ancora in forma di proposta, il considerando n. 24, poi riformato sul punto, prevedeva l'esercitabilità dei diritti dell'interessato solamente in forma individuale e la non delegabilità alla cooperativa di dati[74]. Entrambi tali aspetti sono stati rivisti nel testo definitivo del Regolamento europeo, in cui sono stati espunti. Nella nuova formulazione del corrispondente considerando, contrassegnato ora con il n. 31, si trova affermato che "le cooperative di dati mirano a raggiungere una serie di obiettivi, in particolare a rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri del gruppo, o trovando possibili soluzioni alle posizioni contrastanti dei singoli membri di un gruppo in merito alle modalità di utilizzo dei dati laddove tali dati riguardino più interessati all'interno di tale gruppo. In tale contesto è importante riconoscere che i diritti a norma del regolamento (UE) 2016/679 sono diritti personali dell'interessato e che quest'ultimo non può rinunciarvi (…)".

L'irrinunziabilità dei diritti dell'interessato, pacificamente riconosciuta, è cosa ben diversa dalla loro non delegabilità: anzi, il *revirement* del legislatore europeo sulla formulazione del considerando in esame e le funzioni di *empowerment* dei diritti dell'interessato affidate all'intermediario

diagnosi, alla prognosi, ai benefici e ai rischi degli accertamenti diagnostici e dei trattamenti sanitari indicati, nonché riguardo alle possibili alternative e alle conseguenze dell'eventuale rifiuto del trattamento sanitario e dell'accertamento diagnostico o della rinuncia ai medesimi. *Può* rifiutare in tutto o in parte di ricevere le informazioni ovvero *indicare i familiari o una persona di sua fiducia incaricati di riceverle e di esprimere il consenso in sua vece se il paziente lo vuole*. Il rifiuto o la rinuncia alle informazioni e l'eventuale indicazione di un incaricato sono registrati nella cartella clinica e nel fascicolo sanitario elettronico".

71. Si noti che la legge n. 219/2017 si colloca proprio nell'ottica del trattamento sanitario e non del trattamento dei dati di carattere sanitario, anche se v'è un evidente collegamento tra questi, ad esempio sul piano del diritto a ricevere le informazioni nell'ambito della relazione di cura e a delegare altri a riceverle in propria vece. Che i due piani siano distinti lo si comprende bene sul versante del consenso: il consenso informato di cui all'art. 1 della predetta legge è il consenso informato al trattamento di carattere sanitario sul paziente, che comprende anche il diritto al rifiuto della cura, mentre il consenso informato in materia di protezione dei dati personali riguarda l'autorizzazione ad eseguire operazioni di trattamento dei dati personali per le finalità legittime, esplicite e determinate, stabilite dal titolare del trattamento e comunicate all'interessato nell'informativa *ex* art. 13 (e 14) del GDPR.

72. Si veda, a tale riguardo, Bravo 2023-a.

73. Bravo 2024, Palladini-Scagliarini 2024; Tampieri 2024; Faillace 2024; Proietti 2024; Rufo 2024.

74. Il testo del considerando n. 24 della Proposta di regolamento in materia di governance dei dati (*Data Governance Act*) prevedeva espressamente che " Le cooperative di dati mirano a rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati o risolvendo potenziali controversie tra membri di un gruppo sulle modalità di utilizzo dei dati quando tali dati riguardano più interessati all'interno di tale gruppo. *In tale contesto è importante riconoscere che i diritti a norma del regolamento (UE) 2016/679 possono essere esercitati soltanto a titolo individuale e non possono essere conferiti o delegati a una cooperativa di dati.* Le cooperative di dati potrebbero altresì rappresentare uno strumento utile per imprese individuali, microimprese e piccole e medie imprese che in termini di conoscenze in materia di condivisione dei dati sono spesso equiparabili ai singoli individui".

lasciano supporre l'ammissibilità dell'attribuzione di poteri di rappresentanza volontaria alla cooperativa di dati e, in generale, all'intermediario di dati (anche ove non svolgesse la propria attività in forma cooperativa)[75].

Sull'ammissibilità della delega – ed in particolare nei confronti di persone giuridiche – si è espresso, nel tempo, anche il Garante per la protezione dei dati personali. In un caso concernente un'associazione sportiva, nell'ambito di una fattispecie relativa alla pubblicazione di elenchi, l'*Authority* aveva affermato che "non è ipotizzabile, né previsto dalla legge (...) un diritto dell'associazione ad esercitare i diritti che rientrano nella personale disponibilità di ciascun interessato, a meno che essa possa dimostrare l'esistenza di una specifica *delega* da parte del singolo associato"[76].

Anche più recentemente, sotto l'egida del GDPR, è stata più volte confermata dal Garante l'ammissibilità della delega per l'esercizio dei diritti dell'interessato, ad esempio là dove ha precisato che "la disciplina in materia di protezione dei dati personali prevede – in ambito sanitario – che le informazioni sullo stato di salute devono essere comunicate all'interessato e possono essere comunicate a terzi solo sulla base di un idoneo presupposto giuridico o su indicazione dell'interessato stesso previa *delega* scritta di quest'ultimo (art. 9 Regolamento e art. 83 del Codice in combinato disposto con l'art. 22, comma 11, d.lgs. 10 agosto 2018, n. 101; cfr. anche provv. generale del 9 novembre 2005, doc. web n. 1191411, ritenuto compatibile con il suddetto Regolamento e con le disposizioni del decreto n. 101/2018; cfr. art. 22, comma 4, del citato d.lgs. n. 101/2018)"[77].

75. Attenta dottrina ha affermato che "Sebbene gli esercizi di esegesi delle norme di matrice europea sulla base delle categorie del diritto interno debbano sempre essere condotti con grande prudenza, sembrerebbe ragionevole ritenere che mentre il divieto della rinunzia, quale tipico atto abdicativo, implichi l'impossibilità del conferimento in società (atto con efficacia reale), esso non preclude invece la stipula di un contratto di *mandato (con rappresentanza*), in quanto atto con mera efficacia obbligatoria. Sembrerebbe quindi aprirsi un più ampio spazio operativo quanto meno per la *tutela esterna dei diritti degli interessati da parte di una cooperativa di dati che operi come rappresentante dei suoi membri*". Così Resta 2022. Nella *Joint Opinion n. 3/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act*), 2021, p. 35, l'EDPB e l'EDPS mostravano invero di condividere il principio di non delegabilità dei diritti dell'interessato (esplicitato nel citato considerando n. 24 della proposta di Regolamento sulla governance europea dei dati), mettendo in rilievo la contraddizione di tale principio con le norme che attribuivano alla cooperativa dei dati il potere di negoziare termini e condizioni di maggior vantaggio per gli interessati. La scelta finale del legislatore europeo è stata però quella di comporre la contraddizione facendo salva la negoziabilità ad opera delle *data cooperatives* ed eliminando, al contempo, ogni riferimento al divieto di delega. Quest'ultima, dunque, è da ritenersi pienamente ammissibile in materia di protezione dei dati personali; ciò non solo per le considerazioni che attengono al ripensamento del legislatore europeo nel passaggio dalla proposta al testo definitivo del regolamento, ma anche per ragioni di carattere sistematico.

76. Garante per la protezione dei dati personali, nota del 30 novembre 1999, doc. web n. 1164456.

77. In questo senso v. Garante per la protezione dei dati personali, Provvedimento del 29 aprile 2021, n. 174, doc. web n. 9676143. La delega è stata ritenuta ammissibile anche per la prestazione del reclamo al Garante in luogo dell'interessato: si veda, in tal senso, il provvedimento del Garante n. 209 del 12 maggio 2022, doc. web n. 9790093, ove l'Autorità di settore si è pronunciata sul " (...) reclamo presentato al Garante, ai sensi dell'art. 77 del Regolamento, in data 10 maggio 2020 con il quale XX, su *delega* del fratello XX residente all'estero al momento della presentazione del reclamo, ha chiesto di ordinare a Google LLC la rimozione dai risultati di ricerca reperibili in associazione al nominativo del fratello di due URL che riportano una notizia risalente al 2017 relativa ad un procedimento penale che ha riguardato il reclamante per un fatto avvenuto nella città canadese di XX". Si noti che il GDPR, all'art. 80, par. 1, prevede espressamente che l'interessato abbia "il diritto di dare *mandato* a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto i diritti di cui agli artt. 77, 78 e 79 nonché, se previsto dal diritto degli Stati membri, il diritto di ottenere il risarcimento di

Ulteriore casistica in tema di delega è stata trattata con maggior incertezza da parte del Garante, proprio in tema di intermediazione di dati, con riguardo al caso Hoda e alla fornitura del servizio Weople, di cui s'è già dato conto sopra[78].

5. Intermediazione di dati in ambito sanitario, *European Health Data Space* e regolazione di mercato

L'intermediazione di dati in ambito sanitario è fenomeno che trova la sua manifestazione a prescindere dalla regolamentazione di spazi di dati sanitari di cui al Regolamento (UE) 2025/327[79].

Può considerarsi, innanzitutto, il *data altruism*, che, sin dalla definizione contenuta nel *Data Governance Act*, è preordinato ad alimentare, *inter alia*, il flusso di dati dell'assistenza sanitaria, da inquadrare nell'ambito dell'uso primario dei dati gestiti con l'EHDS, ma anche le ulteriori finalità rilevanti per l'uso secondario, quale la ricerca scientifica e l'elaborazione di politiche pubbliche in ambito sanitario[80].

V'è poi da considerare l'*intermediazione dei dati, svolta in forma cooperativa*, in ambito sanitario[81], ove ad esempio sia posta in essere da pazienti che, con l'aggregazione dei propri dati, possono trarre utilità valorizzabile su differenti piani, incluso quello della ricerca in ambito farmaceutico[82] o nelle relazioni di cura[83]. Il fenomeno tende a creare dei "micro" spazi di condivisione di dati sanitari, con aggregatori di dati che possono essere utilizzati a beneficio dei propri membri con scopo mutualistico e destinati alla loro valorizzazione, con dinamiche gestorie e di controllo sui dati che, nell'intermediazione cooperativa, sono improntate a democraticità e al diretto coinvolgimento degli interessati[84].

Si pensi ancora all'intermediazione di dati sanitari provenienti da intermediari che gestiscono dispositivi biomedicali o strumenti *wearable* ed

cui all'articolo 82". La norma *de qua* non è stata considerata di ostacolo, secondo l'interpretazione del Garante, per l'ammissibilità del reclamo ad opera del fratello dell'interessato su *delega* di quest'ultimo, al fine di esercitare il corrispondente diritto.

78. Si veda anche, *amplius*, Bravo 2025.

79. Il riferimento è ai tre ambiti di intermediazione sostanziale delineati dal *Data Governance Act*: quello relativo al riuso dei dati detenuti da soggetti pubblici; quello relativo alla fornitura di servizi di intermediazione di dati in forma cooperativa e non cooperativa; quello relativo al *data altruism*. Che in tutti e tre gli ambiti si tratti di fenomeni di *data intermediation*, a prescindere dalle etichette usate dal legislatore europeo, è argomento che è stato affrontato in Bravo 2022, a cui *amplius* si rinvia.

80. L'"altruismo dei dati", infatti, viene definitivo, all'art. 2, par. 1, n. 16), del *Data Governance Act*, come "la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, *per obiettivi di interesse generale*, stabiliti nel diritto nazionale, ove applicabile, *quali l'assistenza sanitaria*, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale".

81. Per l'esplorazione di una casistica si veda Rufo 2024, con riferimento ai casi Savvy Cooperative, MIDATA, Salus.Coop, LunaDNA.

82. Si veda, a tal riguardo, De Vico 2024.

83. Anche al di fuori del modello di *data cooperatives* la valorizzazione di aggregazione di dati da parte di comunità di pazienti può seguire percorsi significativi. Si rimanda, ad esempio, alle riflessioni di una decina di anni orsono, esternate in tema di *communities* socio-sanitarie su piattaforme di social network: Bravo 2015.

84. Bravo 2023-a. Si veda anche Palladini-Scagliarini 2024, là dove viene affermato che, con le "cooperative di dati, il legislatore europeo sembra aver colto l'esigenza di affiancare al singolo interessato enti collettivi capaci non solo di assisterlo, come potrebbe fare anche un soggetto terzo, ma anche di permettergli di farsi parte attiva dell'organizzazione e del funzionamento dell'ente, contribuendo ad una forma di rappresentanza e tutela mutualistica di un interesse comune ad altri soggetti cui i dati intermediati si riferiscono".

altri dati che possono avere rilevanza sia sul piano dell'assistenza sanitaria, sia su quello della ricerca (o comunque del *secondary use*), anche in relazione all'acquisizione dei c.d. *real world data*[85].

Si tratta di dati che potrebbero alimentare l'EHDS mediante gli istituti previsti dal nuovo Regolamento e, tra questi, anche mediante il "Diritto delle persone fisiche di inserire informazioni nella propria cartella clinica elettronica" di cui all'art. 5, esercitabile anche tramite rappresentanti[86].

L'intermediazione di soggetti pubblici, che siano detentori di dati appartenenti a particolari categorie e che intendano destinarli al riuso ai sensi del Capo II del *Data Governance Act*, ove operanti in ambito sanitario, finiscono invece per essere istituzionalizzati nel sistema di trattamento delineato con lo spazio europeo di dati sanitari. Si noti però che in tale ambito, ai sensi dell'art. 51 del Reg. EHDS, tali soggetti sono obbligati a rendere disponibili i predetti dati anche per l'uso secondario, diversamente da quanto invece previsto nel DGA, che lascia agli enti pubblici una facoltà (non già un obbligo) di riuso dei dati, rientranti in particolari categorie, da questi detenuti[87].

Leggendo con attenzione il testo dei considerando e quello dell'articolato normativo del predetto Regolamento, ci si può rendere conto che, per gli spazi di condivisione di dati sanitari, il legislatore europeo ha voluto fare riferimento esplicito all'intermediazione dei dati, e ciò merita di essere considerato soprattutto per le implicazioni di sistema, in special modo con riguardo ai "dati sanitari elettronici personali", da intendersi come "i dati relativi alla salute e i dati genetici che sono trattati in formato elettronico"[88].

A seguito della considerazione che gli "Stati membri dovrebbero designare autorità di sanità digitale competenti per la pianificazione e l'attuazione di norme per l'accesso ai dati sanitari elettronici e per la loro trasmissione, nonché per l'applicazione dei diritti delle persone fisiche e dei professionisti sanitari, sotto forma di autorità separate o come parte di autorità già esistenti (…)"[89], il nuovo Regolamento indica quali competenze e quali attività spettano loro, rimarcando anche che sono tenute all'adozione di "*soluzioni di intermediazione* e portali per i pazienti"[90].

85. Liu-Panagiotakos 2022.

86. L'art. 5 cit. del Reg. EHDS stabilisce che "Le persone fisiche o i loro rappresentanti di cui all'articolo 4, paragrafo 2, hanno il *diritto di inserire informazioni* nella propria cartella clinica elettronica attraverso servizi o applicazioni di accesso ai dati sanitari elettronici collegati a tali servizi come indicato al medesimo articolo. *Le informazioni inserite dalla persona fisica o dal suo rappresentante sono chiaramente distinguibili come tali*. Le persone fisiche o i loro rappresentanti di cui all'articolo 4, paragrafo 2, non hanno la possibilità di modificare direttamente i dati sanitari elettronici e le relative informazioni inseriti dai professionisti sanitari".

87. Chiaro è, a tal riguardo, l'art. 5, par. 1, del DGA, ove si prevede che "Gli enti pubblici che, a norma del diritto nazionale, hanno facoltà di concedere o negare l'accesso per il riutilizzo di una o più delle categorie di dati di cui all'articolo 3, paragrafo 1, rendono pubbliche le condizioni per consentire tale riutilizzo nonché la procedura di richiesta del riutilizzo attraverso lo sportello unico di cui all'articolo 8. Qualora concedano o neghino l'accesso per il riutilizzo, possono essere assistiti dagli organismi competenti di cui all'articolo 7, paragrafo 1".

88. Art. 2, par. 2, lett. a), del Reg. EHDS.

89. Considerando n. 30 del Reg. EHDS, il quale prosegue precisando che "(…) Nella maggior parte degli Stati membri esistono già autorità di sanità digitale che si occupano di cartelle cliniche elettroniche, interoperabilità, sicurezza o normazione. Nello svolgimento dei loro compiti, le autorità di sanità digitale dovrebbero cooperare in particolare con le autorità di controllo istituite a norma del regolamento (UE) 2016/679 e con gli organismi di vigilanza istituiti a norma del regolamento (UE) n. 910/2014. Le autorità di sanità digitale possono inoltre cooperare con il comitato europeo per l'intelligenza artificiale istituito dal regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, il gruppo di coordinamento per i dispositivi medici istituito dal regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, il comitato europeo per l'innovazione in materia di dati istituito a norma del regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio e le autorità competenti ai sensi del regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio (…)".

90. Segnatamente, l'indicazione è contenuta nel considerando n. 32, in cui si trova affermato che "Le autorità di sanità digitale dovrebbero avere competenze tecniche sufficienti, riunendo possibilmente esperti di differenti

Non viene però chiarito a quali soluzioni, nello specifico, si faccia riferimento, con ciò lasciando le predette autorità maggiormente libere di indirizzarsi verso le soluzioni che maggiormente soddisfino le esigenze, attingendo eventualmente a modelli già sperimentati o definiti nell'esperienza giuridica europea.

Nel Regolamento EHDS l'intermediazione di dati sanitari viene considerata anche con riguardo allo snellimento degli oneri amministrativi e per giungere a soluzioni di maggior efficacia ed efficienza, qualora vi siano soggetti pubblici o privati che ricevano finanziamenti pubblici, da fonti nazionali o europee, "per raccogliere e trattare dati sanitari elettronici per la ricerca, le statistiche sia ufficiali che non ufficiali, o altre finalità simili, anche in ambiti in cui la raccolta di tali dati è frammentata o difficile, quali quelli relativi alle malattie rare o al cancro"[91]. In tal caso, "al fine di massimizzare l'impatto dell'investimento pubblico e sostenere la ricerca, l'innovazione, la sicurezza dei pazienti o la definizione delle politiche, a beneficio della società"[92], siffatti dati "dovrebbero essere messi a disposizione degli organismi responsabili dell'accesso ai dati sanitari (…)"[93], in ragione del fatto che vengono "raccolti e trattati dai titolari dei dati sanitari con il sostegno di finanziamenti pubblici nazionali o dell'Unione"[94]. In tale contesto, nella consapevolezza che ciò possa tradursi in un aggravio di oneri amministrativi o in un affaticamento dell'ordinaria attività, che finirebbe per perdere anche solo in parte la sua efficacia o la sua efficienza, il legislatore eurounitario ha ritenuto di accordare agli Stati membri la facoltà di prevedere, nell'ordinamento nazionale, che, "per talune categorie di titolari di dati sanitari[95], le *funzioni* siano

organizzazioni. Le attività di tali autorità dovrebbero essere ben pianificate e monitorate al fine di garantirne l'efficienza. Le autorità di sanità digitale dovrebbero adottare le misure necessarie per proteggere i diritti delle persone fisiche mettendo a punto soluzioni tecniche nazionali, regionali e locali quali cartelle cliniche elettroniche nazionali, *soluzioni di intermediazione* e portali per i pazienti. È opportuno che, nell'adottare tali misure di protezione necessarie, le autorità sanitarie digitali applichino norme e specifiche comuni in tali soluzioni, promuovano l'applicazione delle norme e delle specifiche negli appalti e utilizzino altri mezzi innovativi come il rimborso di soluzioni conformi alle prescrizioni in materia di interoperabilità e sicurezza dello spazio europeo dei dati sanitari (…)".

91. Considerando n. 59 del Reg. EHDS.
92. *Ibidem*.
93. *Ibidem*.
94. *Ibidem*.
95. Quanto alle categorie di titolari di dati sanitari, il considerando n. 59 cit. fa riferimento sia a soggetti pubblici che a soggetti privati. Viene precisato, a tal riguardo, che "(…) In alcuni Stati membri i soggetti privati, compresi i prestatori di assistenza sanitaria privati e le associazioni professionali, svolgono un ruolo di fondamentale importanza nel settore sanitario. I dati sanitari detenuti da tali prestatori dovrebbero essere resi disponibili anche per l'uso secondario. I titolari dei dati sanitari nel contesto dell'uso secondario dovrebbero pertanto essere soggetti che sono prestatori di assistenza sanitaria o cure assistenziali o svolgono attività di ricerca in relazione ai settori dell'assistenza sanitaria o delle cure assistenziali, o sviluppano prodotti o servizi destinati ai settori dell'assistenza sanitaria o delle cure assistenziali. Tali enti possono essere pubblici, senza scopo di lucro o privati. In linea con tale definizione, le case di cura, i centri di assistenza diurna, i soggetti che forniscono servizi alle persone con disabilità, i soggetti che svolgono le attività commerciali e tecnologiche connesse all'assistenza, come i centri ortopedici e le imprese che forniscono servizi di assistenza, dovrebbero essere considerati titolari di dati sanitari. Anche le persone giuridiche che sviluppano applicazioni per il benessere dovrebbero essere considerate titolari di dati sanitari. Anche le istituzioni, gli organi e gli organismi dell'Unione che trattano tali categorie di dati relativi alla salute e all'assistenza sanitaria nonché i registri di mortalità dovrebbero essere considerati titolari di dati sanitari. Al fine di evitare un onere sproporzionato a loro carico, di norma le persone fisiche e le microimprese dovrebbero essere esentate dagli obblighi dei titolari di dati sanitari. Gli Stati membri dovrebbero tuttavia poter estendere gli obblighi dei titolari di dati sanitari alle persone fisiche e alle microimprese nel loro diritto nazionale (…)".

svolte da *intermediari di dati sanitari*"[96], precisando che "Tali *intermediari di dati sanitari* dovrebbero essere persone giuridiche in grado di trattare, rendere disponibili, registrare, fornire o scambiare dati sanitari elettronici per l'uso secondario forniti da titolari dei dati, o limitarne l'accesso", svolgendo tuttavia "*compiti diversi* da quelli dei *servizi di intermediazione dei dati nell'ambito del regolamento (UE) 2022/868*"[97].

Non appare chiarissimo quale sia il senso della contrapposizione con i servizi di intermediazione di dati di cui al *Data Governance Act*. Si noti, comunque, che la proclamata diversità non riguarda la natura o la qualità soggettiva del fornitore di servizi di intermediazione di dati di cui al predetto regolamento, ma solamente i "compiti", sicché l'intermediario di dati a cui fare eventualmente ricorso potrebbe ben essere anche quello istituito ai sensi di tale disciplina, già dotato di competenze tecniche e know-how per operare correttamente nel settore della *data intermediation*, con una rimodulazione di compiti, da definire nell'ordinamento nazionale a cura degli Stati membri, che dovranno essere ritagliati per le esigenze degli spazi di condivisione dei dati sanitari precisati nel considerando in parola[98].

Vi sono comunque margini per il ricorso all'intermediazione di dati sanitari nell'*European eHealth Data Space*, che passano per il vaglio del legislatore nazionale.

Il ricorso all'intermediazione non è però senza limiti: gli Stati membri, infatti, non possono farvi ricorso per designarli quali "titolari dei dati sanitari affidabili"[99], ossia quali soggetti, designati dagli Stati membri, che possono avvalersi di una "*procedura di rilascio dell'autorizzazione dei dati* [che] può essere eseguita in modo semplificato, al fine di *alleviare l'onere amministrativo a carico degli organismi responsabili dell'accesso ai dati sanitari* nella gestione delle richieste di dati da essi trattati"[100].

Al di fuori dei considerando, in cui l'intermediazione dei dati compare più volte, il Regolamento EHDS mostra cautela nel considerare tale istituto giuridico.

V'è un parco riferimento all'art. 2, par. 2, lett. *k)*, con riguardo alla definizione di "sistema di cartelle cliniche elettroniche", inteso come "qualsiasi sistema in cui il software oppure la combinazione tra l'hardware e il software del sistema consente ai dati sanitari elettronici personali rientranti nelle categorie prioritarie di dati sanitari elettronici personali stabilite a norma del presente regolamento di essere conservati, *intermediati*, esportati, importati, convertiti, modificati o visualizzati e destinato dal fabbricante a essere utilizzato dai prestatori di assistenza sanitaria nel fornire cure assistenziali ai pazienti o dai pazienti nell'accedere ai loro dati sanitari elettronici". L'enunciata *intermediabilità* dei dati sanitari elettronici personali rafforza dunque l'idea che il sistema delineato nel Regolamento EHDS sia improntato alla *data intermediation*, ma di per sé nulla aggiunge in merito alla possibilità di ricorrere a fornitori di servizi di intermediazione diversi dai titolari di dati sanitari: l'intermediabilità dei dati a cui si fa riferimento, infatti, potrebbe essere quella raggiunta mediante il sistema congegnato con la realizzazione dell'*European eHealth Data Space*, che ne permette la circolazione tra soggetti diversi tanto per l'uso primario che per l'uso secondario, e non con il ricorso ad ulteriori servizi di intermediazione di dati.

Diverso è invece l'ulteriore esplicito riferimento all'intermediazione contenuto nell'art. 50 del Reg. EHDS, di apertura del Capo IV, dedicato all'"Uso

96. Considerando n. 59 del Reg. EHDS.

97. *Ibidem*.

98. Come già evidenziato si tratta di esigenze orientate all'alleggerimento degli oneri amministrativi e al mantenimento dell'efficienza e dell'efficacia del sistema.

99. Il divieto è enunciato nella parte finale del considerando n. 76 del Reg. EHDS.

100. Considerando n. 76 del Reg. EHDS, ove si aggiunge che "I titolari dei dati sanitari affidabili dovrebbero essere autorizzati a valutare le domande di accesso ai dati sanitari presentate nell'ambito di questa procedura semplificata, sulla base delle loro competenze nell'affrontare il tipo di dati sanitari che stanno trattando, e di rilasciare una raccomandazione in merito a un'autorizzazione ai dati. L'organismo responsabile dell'accesso ai dati sanitari dovrebbe rimanere responsabile del rilascio dell'autorizzazione finale ai dati e non dovrebbe essere vincolato dalla raccomandazione fornita dal titolare dei dati sanitari affidabile".

secondario", e, in esso, della Sezione 1, intitolata alle "Condizioni generali relative all'uso secondario".

Tale articolo, rubricato "Applicabilità ai titolari dei dati sanitari", enuncia quali categorie di titolari dei dati sanitari siano da considerarsi esonerate dagli obblighi spettanti ai titolari dei dati sanitari con riguardo alla disciplina in tema di uso secondario (e vengono menzionate le persone fisiche, compresi i singoli ricercatori, e le persone giuridiche considerate microimprese), salvo consentire agli Stati membri la facoltà di stabilire, con norme dell'ordinamento nazionale, che gli obblighi in questione siano applicabili anche alle categorie soggettive che il Regolamento europeo ha inteso esonerare[101] oppure che per determinate categorie di titolari dei dati sanitari gli obblighi vengano "assolti da entità di intermediazione di dati sanitari"[102], con la precisazione che "an tal caso, i dati sono comunque considerati come messi a disposizione da vari titolari dei dati sanitari"[103], ai fini del loro uso secondario.

Stante la rilevanza che l'intermediazione di dati ha nelle strategie europee di *data governance*, sinceramente, ci si aspettava di più dal legislatore europeo sul versante dello spazio europeo di dati sanitari, in particolare sul fronte delle dinamiche concorrenziali e degli effetti di regolazione del mercato.

Il sistema delineato nel nuovo regolamento, istitutivo dell'*European Health Data Space* – mediante la previsione di norme e infrastrutture comuni e di un quadro di governance che facili l'accesso ai dati sanitari elettronici per l'uso primario e secondario dei dati sanitari elettronici – costituisce indubbiamente un'ottima innovazione, che enfatizza la prospettiva della circolazione dei dati personali e la loro "funzione sociale", declamata nel GDPR al considerando n. 4[104], e crea indubbiamente i presupposti per un salto di qualità nell'assistenza sanitaria, nella ricerca e nell'innovazione, anche con riguardo allo sviluppo di tecnologie di intelligenza artificiale, che necessitano di dati di addestramento significativi e qualitativamente controllati.

Si ha però l'impressione che tale sistema, centralizzato, venga realizzato in una logica esclusiva ed in gran parte escludente i nuovi *player* del mercato: quegli "intermediari di dati" che il *Data Governance Act*, in attuazione della strategia europea dei dati, aveva voluto affermare, come soluzione europea alle dinamiche di mercato, dominate dalle multinazionali straniere, soprattutto americane (le c.d. *Big Tech*).

Il lodevole intento di realizzare un sistema efficace, centralizzato, di condivisione di dati in ambito sanitario, per come è congegnato, rischia di essere doppiamente escludente se lo si considera nella prospettiva del mercato e delle dinamiche di autodeterminazione informativa dei pazienti.

Per un verso finisce per "tagliare fuori" i nuovi intermediari, che rimangono ai margini del sistema di condivisione dei dati sanitari; per altro verso l'EHDS, nel concentrare l'attenzione sull'uso primario dei dati e nel favorire l'uso secondario per esigenze connesse al pubblico interesse (e a quello commerciale che ruota intorno alla gestione centralizzata del *secondary use*)[105], finisce per "espropriare" sostanzialmente i pazienti della possibilità di controllo e di valorizzazione dei dati, per le dinamiche di uso secondario, escludendoli dalla possibilità di negoziazione sull'uso dei propri dati che, tramite l'intermediario, consentirebbe loro di ottenere vantaggi dagli utenti di dati[106].

101. Art. 50, par. 2, del Reg. EHDS.

102. Art. 50, par. 3, del Reg. EHDS.

103. *Ibidem*.

104. In tale considerando viene precisato che "Il trattamento dei dati personali dovrebbe essere *al servizio dell'uomo*. 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 con altri diritti fondamentali, in ossequio al principio di proporzionalità (…)" (corsivi aggiunti). Sul punto si veda Ricci 2017, nonché Bravo 2023-c.

105. Si pensi allo sviluppo di soluzioni di IA, solo per fare un esempio.

106. Va ricordato ancora una volta che con il servizio di cooperativa di dati, *ex* art. 2, par. 1, n. 15, del *Data Governance Act*, viene a realizzarsi un servizio di intermediazione dei dati offerti da una struttura organizzativa costituita a soggetti che partecipano a tale struttura quali membri e che tale struttura, quale intermediario di dati con finalità mutualistiche, ha come obiettivi principali non solo quelli di aiutare i propri membri nell'esercizio dei

Si ha cioè l'impressione che con l'EHDS l'autorità pubblica si sostituisca d'imperio agli intermediari privati nella realizzazione di un sistema funzionale di condivisione di dati a livello europeo e faccia venir meno, nei confronti degli interessati, quell'utilità che gli stessi avrebbero potuto conseguire facendo uso dell'autonomia privata, ottenendo per sé quei vantaggi che l'intermediazione dei dati gli avrebbe potuto far conseguire[107].

Così come strutturato dal nuovo Regolamento, l'*European Health Data Space*, con riguardo al *secondary use* dei dati dei pazienti, sembra comportare una sorta di depotenziamento degli intermediari dei dati e degli stessi interessati, che, pur beneficiando di sistemi di portabilità evoluti che portano ad un arricchimento, su scala europea, delle possibilità di uso primario dei dati personali, svuotano nei confronti dei privati le possibilità connesse alla governance dei dati sul fronte dell'uso secondario, sterilizzando di fatto la possibilità di una loro diretta valorizzazione. In altre parole, sembra si sia voluto intervenire anche con norme volte a regolamentare, in senso restrittivo, il *data market* in ambito sanitario e il ruolo di intermediazione svolto in tale ambito da operatori privati.

Poiché, come s'è potuto ricostruire in queste pagine, il fenomeno dell'intermediazione, seppur compresso, non pare affatto scomparire nell'impianto del Regolamento, avendo margini di applicazione che sono per lo più rimessi alle scelte del legislatore nazionale e delle autorità competenti chiamate a darne attuazione, si dovrebbero percorrere soluzioni che portino a valorizzare i fenomeni di intermediazione delineati nel *Data Governance Act* ed emergenti sulla base degli strumenti che il GDPR già consente.

Tra le soluzioni percorribili, oltre a quelle che mirino a valorizzare i richiami all'intermediazione dei dati di cui v'è traccia nel Reg. EHDS, sopra passati in rassegna, v'è anche quella che passa per l'applicazione dell'art. 1, par. 8, ai sensi del quale "il presente regolamento lascia impregiudicato l'accesso ai dati sanitari elettronici per l'uso secondario *concordato nel quadro di accordi* contrattuali o amministrativi tra soggetti pubblici o privati".

È forse questa la via che consente, a chi gestisce lo spazio europeo di dati sanitari, di valorizzare il ruolo degli intermediari, ricorrendo ad accordi *ad hoc* per la disciplina dei rapporti, che consentano di preservare, seppur con le garanzie che la particolare natura dei dati imporne a tutela dei diritti degli interessati, le possibilità di controllo e valorizzazione a loro vantaggio, connesse alla gestione del *secondary use* dei dati intermediati.

Riferimenti bibliografici

P. Alberti (2008), *Le vicende soggettive dell'esecutore*, vol. V, *I settori speciali. L'esecuzione*, in "Trattato sui contratti pubblici", diretto da M.A. Sandulli, R. De Nictoli, R. Garofoli, Giuffrè, 2008

G. Alpa (2022), *Solidarietà. Un principio normativo*, il Mulino, 2022

M. Bombardelli (2023), *Le relazioni tra istituzioni pubbliche e mercati*, in Id. (a cura di), "L'intervento amministrativo sui mercati", Giappichellli, 2023

loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, e di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, ma anche quello di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali, ottenendo vantaggi in termini di valorizzazione dei dati, nella concessione dell'uso secondario, che altrimenti il singolo interessato, per difetto di potere contrattuale, non riuscirebbe ad ottenere.

107. In questo senso, la regolazione del mercato in tale ambito specifico, seppur mossa dalla necessità di raggiungere finalità di interesse generale, finisce per creare ingerenze delle istituzioni pubbliche tali da alterare la logica di funzionamento delle dinamiche di mercato, la cui spontaneità si sarebbe invece dovuta preservare. In materia si veda ancora una volta, per l'impostazione di carattere generale, Bombardelli 2023.

F. Bravo (2025), *Intermediazione di dati sanitari e diritto alla portabilità*, in A. Morace Pinelli (a cura di), "Sanità digitale. Regolamento EHDS (UE 2025/327) sullo spazio europeo dei dati sanitari. Vol. 1, Uso dei dati e assetti organizzativi", Pacini, 2025

F. Bravo (a cura di) (2024), *EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo*, Giappichelli, 2024

F. Bravo (2023-a), *Le cooperative di dati*, in "Contratto e impresa", 2023, n. 3

F. Bravo (2023-b), *Il principio di solidarietà*, in Id. (a cura di), "Dati personali. Protezione, libera circolazione e governance. Vol. 1. Principi", Pacini, 2023

F. Bravo (2023-c), *Il principio di solidarietà tra data protection e data governance*, in "Il diritto dell'informazione e dell'informatica", 2023, n. 3

F. Bravo (2023-d), *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione*, in "Contratto e impresa", 2023, n. 2

F. Bravo (2022), *Data Governance Act and Re-Use of Data in the Public Sector*, in "European Review of Digital Administration & Law", vol. 3, 2022, n. 2

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

F. Bravo (2020), *Il commercio elettronico dei dati personali*, in T. Pasquino, A. Rizzo, M. Tescaro (a cura di), "Questioni attuali in tema di commercio elettronico", ESI, 2020

F. Bravo (2019), *Le condizioni di liceità del trattamento di dati personali*, in G. Finocchiaro (a cura di), "La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101", Zanichelli, 2019

F. Bravo (2018), *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Wolters Kluwer-Cedam, 2018

F. Bravo (2017), *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in G. Finocchiaro (a cura di), "Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali", Zanichelli, 2017

F. Bravo (2015), *EHealth e social networks per la realizzazione di communities socio-sanitarie in tema di malattie rare. Riflessioni giuridiche tra diritti fondamentali e responsabilità civile*, in C. Faralli, R. Brighi, M. Martoni (a cura di), "Strumenti, diritti, regole e nuove relazioni di cura. Il paziente europeo protagonista nell'eHealth", Giappichelli, 2015

F. Bravo, J. Valero Torrijos (2022), *Data in the Public Sector and Data Valorisation*, in "European Review of Digital Administration & Law", vol. 3, 2022, n. 2

I. Cardinali (2024), *Tutela degli interessati e esercizio dei diritti: l'efficace intermediazione delle cooperative di dati*, in F. Bravo (a cura di), "EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo", Giappichelli, 2024

A. De Vico (2024), *I servizi di cooperazione di dati nella ricerca clinica farmaceutica: analisi e prospettive*, in F. Bravo (a cura di), "EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo", Giappichelli, 2024

S. Faillace (2025), *Prospettive civilistiche in ordine agli spazi di condivisione dei dati sanitari alla luce del Regolamento EHDS*, Wolters Kluwer, 2025

S. Faillace (2024), *Le cooperative di dati sanitari tra codice civile e Data Governance Act*, in F. Bravo (a cura di), "EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo", Giappichelli, 2024

F. Galgano (2014), *Trattato di diritto civile*, Wolters Kluwer-Cedam, 2014 (3a ed. agg. a cura di N. Zorzi Galgano, vol. II)

J. Hagel, J.F. Rayport (1997-a), *The Coming Battle for Customer Information*, in "Harvard *Business* Review", 1997, January-February

J. Hagel, J.F. Rayport (1997-b), *The new infomediaries*, in "The McKinsey Quarterly", 1997, Autumn

G. Iudica (2009), *Il contratto di appalto*, in N. Lipari, P. Rescigno (diretto da), "Diritto civile", vol. III, Giuffrè, 2009

U. Izzo, P. Guarda (2010), *Sanità elettronica, tutela dei dati personali e digital divide generazionale: ruolo e criticità giuridica della delega alla gestione dei servizi di sanità elettronica da parte dell'interessato*, Università di Trento, 2010

T. Lester (2001), *The Reinvention of Privacy*, in "The Atlantic", 2001, March

F. Liu, D. Panagiotakos (2022), *D. Real-world data: a brief review of the methods, applications, challenges and opportunities*, in "BMC Med Res Methodol", vol. 22, 2022, n. 287

G. Miele (1962), voce *Delega (dir. amm.)*, in "Enciclopedia del diritto", vol. XI, Giuffrè, 1962

A. Morace Pinelli (a cura di) (2025), *Sanità digitale. Regolamento EHDS (UE 2025/327) sullo spazio europeo dei dati sanitari*. Vol. 1, *Uso dei dati e assetti organizzativi*, Pacini, 2025

A. Morace Pinelli (a cura di) (2024), *Dalla "Data Protection" alla "Data Governance": il regolamento (UE) 2022/868. Commentario al "Data Governance Act"*, Pacini, 2024

G. Musolino (2011), *Comm. sub art. 1656 c.c.,* in D. Valentino (a cura di), "Dei singoli contratti, Vol. II, Artt. 1655-1802 c.c.", nel Commentario al Codice Civile diretto da E. Gabrielli, Utet, 2011

V. Palladini, S. Scagliarini (2024), *Le cooperative di dati come forma di tutela collettiva degli interessati: un'opportunità per l'ambito sanitario?*, in F. Bravo (a cura di), "EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo", Giappichelli, 2024

L. Petrone (2023), *Il mercato digitale europeo e le cooperative di dati*, in "Contratto e impresa", 2023, n. 3

D. Poletti (2024), *Il quadro normativo del "Data Governance Act": l'esercizio dei diritti dell'interessato nell'attività di intermediazione dei dati*, in "Nuove leggi civili commentate", 2024, n. 3

D. Poletti (2022), *Gli intermediari dei dati*, in "European Journal of Privacy Law & Technologies", 2022, n. 1

G. Proietti (2024), *Cooperative di dati, Spazio europeo dei dati sanitari e Data Act nel dedalo normativo*, in F. Bravo (a cura di), "EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo", Giappichelli, 2024

G. Resta (2022), *Pubblico, privato e collettivo nel sistema europeo di governo dei dati*, in "Rivista trimestrale di diritto pubblico", 2022, n. 4

G. Resta, V. Zeno Zencovich (a cura di) (2023), *Governance of/through data*, Roma Tre Press, 2023

G. Resta, V. Zeno Zencovich (2018), *Volontà e consenso nella fruizione dei servizi in rete*, in "Rivista trimestrale di diritto e procedura civile", 2018, n. 2

A. Ricci, A. Spangaro (2024), *La tutela dell'interessato nell'economia dei dati: il ruolo delle cooperative di dati*, in F. Bravo (a cura di), "EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo", Giappichelli, 2024

A. Ricci (2017), *Sulla "funzione sociale" del diritto alla protezione dei dati personali*, in "Contratto e impresa", 2017, n. 2

S. Rodotà (2014), *Solidarietà. Un'utopia necessaria*, Laterza, 2014

L. Rufo (2024), *Data Governance Act e cooperative di dati: una "possibile" nuova frontiera per la ricerca in sanità*, in F. Bravo (a cura di), "EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo", Giappichelli, 2024

M. Tampieri (2024), *Cooperative di dati per la tutela della salute*, in F. Bravo (a cura di), "EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo", Giappichelli, 2024

S. Troiano (2019), *Il diritto alla portabilità dei dati*, in N. Zorzi Galgano (a cura di), "Persona e mercato dei dati. Riflessioni sul GDPR", Wolters Kluwer-Cedam, 20219

V. Zeno Zencovich (2019), *Do "Data Markets" Exist?*, in "MediaLaws", 2019, n. 2

V. Zeno Zencovich (2018), *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in "Media Laws", 2018, n. 2

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0260 • articolo sottoposto a peer review • pubblicato in anteprima il 19 gen. 2026

Matteo Falcone

I dati aperti come strumento di regolazione del mercato digitale tra vecchie e nuove prospettive

La disciplina dei dati aperti è oramai pienamente uno strumento per regolare i mercati digitali, attraverso la de-strutturazione degli oligopoli privati. Recentemente è oggetto di una evoluzione interessante: da disciplina per superare il paradigma proprietario sui dati da parte delle amministrazioni, sta diventando progressivamente un paradigma generale, che si applica anche ai dati in possesso dei soggetti privati. L'obiettivo di questo lavoro, dunque, dopo aver ricostruito in sommi capi la disciplina dei dati aperti come strumento di regolazione del mercato unico europeo, è quello di fare emergere qualche elemento critico. In primo luogo in merito all'impostazione normativa europea, in particolare rispetto alle finalità originarie sottese alla filosofia degli open data. Inoltre, in merito al ruolo che hanno (e che, invece, dovrebbero avere) le amministrazioni pubbliche in questo contesto normativo.

Open data – Mercato digitale – Data act – Data governance act – Beni comuni

Open data as a regulatory tool for the digital market across traditional and emerging perspectives

The regulation of open data has now fully matured into a key instrument for regulating digital markets, primarily by disrupting private oligopolies. Recently, it has undergone a compelling evolution: originally conceived as a framework to move beyond the proprietary control of data by public administrations, it is progressively becoming a general paradigm that also applies to data held by private entities. The objective of this analysis is therefore – after briefly outlining the open data framework as a regulatory tool for the European Single Market – to highlight certain critical aspects. This critique focuses, first, on the European legislative approach, particularly in relation to the original objectives underpinning the philosophy of open data. Second, it addresses the role currently performed (and the role that should instead be adopted) by public administrations within this evolving regulatory landscape.

Open data – Digital market – Data act – Data governance act – Commons

L'Autore è dottore di ricerca in Diritto amministrativo e docente di Diritto dell'informazione e della comunicazione presso Università degli studi di Perugia

Questo contributo fa parte della sezione monografica *I dati in ambito pubblico tra esercizio della funzione amministrativa e regolazione del mercato*, a cura di Marco Bombardelli, Simone Franca, Anna Simonati

1. Introduzione

Nell'annoso processo di progressiva "europeizzazione" della disciplina sulla circolazione dei dati[1], gli open data sono divenuti un importante strumento di rafforzamento del mercato unico europeo e – allo stesso tempo, anche se ancora *in nuce* – potrebbero diventare un paradigma generale di circolazione dei dati nell'Unione europea.

Da un lato, l'entrata in vigore delle norme europee più recenti – in particolare del *Data governance Act* e del *Data Act* – hanno chiarito definitivamente come la principale finalità della circolazione dei dati in possesso delle amministrazioni pubbliche sia quella di rafforzare il mercato unico europeo. L'obiettivo del legislatore è quello di permettere alle imprese – soprattutto piccole e medie – di sviluppare nuovi prodotti attraverso i dati aperti e di guadagnarsi ulteriori spazi di mercato, in particolare nei mercati digitali.

Dall'altro lato, invece, queste norme hanno aperto nuove (ed interessanti) prospettive sui soggetti a cui si applicano forme di "apertura" dei dati. Il paradigma dei dati aperti, che nasceva per rompere il regime proprietario delle amministrazioni pubbliche sui dati in loro possesso, oggi potrebbe assumere una valenza più generale, in quanto sta cominciando, anche se solo in casi eccezionali e a determinate condizioni, a mettere in discussione anche l'approccio proprietario dei soggetti privati sui dati in loro possesso. Una disciplina che mira a "democratizzare" l'utilizzo dei dati di interesse pubblico[2], al di là della loro titolarità, provando a de-strutturare i preoccupanti oligopoli privati che

1. Sottolinea diffusamente questo aspetto Carloni 2025 e già Cortese 2021. La crescita delle norme europee sulla digitalizzazione, in particolare sui dati, è descritta molto bene in Lobascio 2023.
2. Come si chiarirà anche più avanti, sta emergendo dalle norme europee una più generale e trasversale categoria di dati di interesse pubblico. Una ipotesi già presente nella Comunicazione della Commissione, *Costruire un'economia dei dati europea*, COM/2017/9 final, nella Commission Staff, *Working Document on the free flow of data and emerging issues of the European data economy*, SWD (2017) 2 final e, infine, nella più nota

si sono formati progressivamente nei mercati *data-based*, proprio grazie al possesso e all'utilizzo massivo (ed esclusivo) di questi dati[3]. Una disciplina che, da quest'ultimo punto di vista, va affiancata e "letta" insieme a quella più direttamente dedicata alla tutela della concorrenza nei mercati digitali[4], ma che già di per sé istituisce un importante istituto pro-concorrenziale, a cui però andrebbe affidata una maggiore capacità prescrittiva ed impositiva, qualora si volesse davvero "aprire" le banche dati private a fini democratici.

L'obiettivo di questo lavoro, dunque, è quello di ricostruire per sommi capi la disciplina dei dati aperti come strumento di regolazione del mercato unico europeo e di fare emergere qualche elemento critico sia in merito all'impostazione normativa europea, in particolare rispetto alle finalità originarie sottese alla filosofia degli *open data*, sia in merito al ruolo che hanno (e che, invece, dovrebbero avere) le amministrazioni pubbliche in questo contesto normativo.

2. La filosofia dei dati aperti e le sue finalità

Prima di entrare nel merito della disciplina vigente è utile esplicitare la logica, in particolar modo le finalità che originariamente hanno caratterizzato la filosofia degli *open data* e che hanno contribuito alla sua diffusione e alla sua rilevanza nella società contemporanea.

La filosofia dei dati aperti rappresenta, di fatto, l'applicazione della teoria dei *commons* ai dati in possesso delle amministrazioni. Come è noto, alla base di questa teoria c'è il tentativo di ripensare il regime proprietario dei beni, affiancando alle categorie dei beni pubblici e dei beni privati, quella dei beni comuni, per garantire a tutti il godimento di beni ritenuti "essenziali" per l'esercizio dei diritti fondamentali. La teoria dei *commons*, in sostanza, assicura il godimento di questi diritti attraverso lo sganciamento dei due attributi fondamentali del diritto di proprietà, cioè la titolarità, che resta pubblica o privata, dall'accesso al bene "essenziale", che è consentito a tutti coloro che vogliono utilizzarlo per esercitare i loro diritti fondamentali[5].

Coerentemente con questo approccio, la filosofia degli open data teorizza lo sganciamento della titolarità dei dati pubblici, che continuano ad essere in possesso delle amministrazioni, dall'accesso ai dati, da garantire a chiunque in modo libero e gratuito. Un accesso che permetta, inoltre, il loro riutilizzo, senza particolari condizioni in termini di finalità e senza imposizione di determinate modalità[6].

Comunicazione *Una strategia europea per i dati*, COM/2020/66 final, le quali fanno riferimento al concetto di "dati per il bene pubblico".

3. La crescita esponenziale dei dati utilizzabili e lo sviluppo di una capacità computazionale senza precedenti hanno prodotto una vera egemonia computazionale dei poteri privati, la quale sta ribaltando il paradigma per cui la conoscenza sia uno strumento appannaggio solo del potere pubblico. In questo senso si permetta di richiamare Falcone 2023. Sui poteri privati digitali in generale si v. Cremona 2023, Betzu 2022, Betzu 2021, Pardolesi 2021.
4. Ci riferiamo al Regolamento (UE) 2022/1925 del Parlamento Europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale, il c.d *Digital Market Act*. La letteratura scientifica sul punto oramai è cospicua. Per una lettura giuspubblicistica si v. Pollicino 2023, mentre per una disamina generale del contenuto del regolamento e sui suoi effetti sul diritto antitrust si v. Licastro 2025. Un regolamento che lascia comunque importanti "vuoti" di regolazione, i quali contribuiscono paradossalmente a lasciare inalterate, se non addirittura a peggiorare, alcune concentrazioni di mercato. In questo senso si v. Simone–Laudando 2025 e Kurz 2023.
5. Sulla teoria dei *commons* la letteratura è sconfinata. Solo per indicare i lavori italiani più esemplificativi si v. Marella 2017; Rodotà 2013; Marella 2012; Mattei 2011. Inoltre, il paragrafo 2 di Di Masi 2022. Anche la letteratura giuspubblicistica si è occupata del tema. Si v. Donati 2024, Renna–Micciché 2022, Cerulli Irelli 2022, Arena 2022, Bombardelli 2016, Cortese 2016, Ciervo 2013.
6. Mette bene in evidenza come questa disarticolazione tra la titolarità dei dati pubblici e il loro riutilizzo sia il nucleo centrale della concezione dei dati come *commons*, Marongiu 2008, Ponti 2007, D'Elia 2006. Per una recente riflessione sulla disarticolazione della titolarità dall'accesso ai dati personali si v. Simonati 2025.

Questo perché la natura dei dati pubblici e le modalità della loro raccolta e produzione giustificherebbero l'applicazione della teoria dei *commons*. I dati in possesso delle amministrazioni, come tutti i beni pubblici, sono beni non rivali (cioè beni il cui consumo da parte di un individuo non impedisce né riduce la possibilità di consumo da parte di altri individui)[7] e sono raccolti da poteri e con risorse pubbliche (in particolare dalle amministrazioni pubbliche, che qui intendiamo in senso ampio), per l'esercizio di una funzione amministrativa, dunque per il raggiungimento di una finalità di interesse pubblico.

Per questi due motivi principali, i dati pubblici non possono essere considerati come dei beni di proprietà delle amministrazioni, ma sono un patrimonio della collettività – non solo (e banalmente) in quanto beni alla cui raccolta e produzione i cittadini hanno già contribuito con il loro concorso alla fiscalità generale (tramite imposte e tasse), che finanzia le attività amministrative – ma perché la produzione di nuova conoscenza che essi garantiscono li rende "essenziali" per la realizzazione di importanti interessi collettivi e per l'esercizio dei diritti fondamentali. Di conseguenza, il compito delle amministrazioni, dopo averli utilizzati per le finalità di esercizio della funzione (che sarebbero, di fatto, le loro prime finalità di utilizzo), sarebbe quello di curarne la qualità e di metterli a disposizione della collettiva proprio per l'esercizio di questi diritti o per la cura di determinati interessi collettivi[8].

Il primo interesse collettivo a cui i dati aperti sono preposti è sicuramente lo sviluppo economico o, in termini più individualistici, la libertà di iniziativa economica. Nella filosofia dei dati aperti entrambi vengono declinati in termini più ampi rispetto al paradigma del mero riutilizzo dei dati – che, ad esempio, aveva costituito la ratio della prima disciplina europea[9]. A differenza del riutilizzo – in cui la valorizzazione dei dati pubblici garantiva un ritorno economico alle amministrazioni pubbliche, in quanto potevano rilasciare, di fatto, i dati in proprio possesso anche ad un costo comprensivo di un margine di profitto – nel paradigma dei dati aperti, la valorizzazione economica dei dati pubblici è a vantaggio dei soggetti privati, che riutilizzano liberamente e gratuitamente i dati pubblici[10]. La loro libera circolazione, dunque, diventa uno strumento per favorire lo sviluppo economico e la libera iniziativa economica dei cittadini, in quanto, sulla base dei dati aperti, i soggetti privati possono sviluppare e offrire nuovi e più innovativi servizi *databased* ad altri soggetti privati, ma anche alle stesse amministrazioni pubbliche[11].

Inoltre, la filosofia degli open data affianca a questo primo interesse altri due diritti a cui i dati aperti sarebbero legati, entrambi strumentali alla più generale garanzia della democraticità delle decisioni pubbliche: i diritti di partecipazione dei cittadini ai processi decisionali pubblici e l'interesse generale al controllo democratico delle decisioni pubbliche, attraverso la trasparenza amministrativa.

7. I dati pubblici, ma, in generale, i dati sono beni non rivali in quanto beni immateriali. Per una disamina precisa sui caratteri dei dati pubblici si v. Ponti 2008 e la bibliografia ivi riportata.
8. Sulla filosofia degli open data e sulle sue giustificazioni si v. per tutti Van Maanen–Ducuing–Fia 2024, Purtova–van Maanen 2023, Solda-Kutzman 2011, in particolare la ricostruzione teorica ivi riportata. Sui dati aperti nelle amministrazioni pubbliche italiane, invece, si v. Carloni 2022, Rossa 2021, Carullo 2019, Galetta 2019, Simonati 2018, Di Mascio 2017, Falcone 2016, Costantino 2015, Carloni 2014, Ponti 2013, Bonomo 2012.
9. Ci si riferisce alla direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, relativa al riutilizzo dell'informazione del settore pubblico e alla sua attuazione italiana. Per tutti si v. ancora Marongiu 2008, Ponti 2007, D'Elia 2006.
10. Per un approfondimento sulla differenza che intercorre tra il riutilizzo e la filosofia dei dati aperti si permetta di richiamare Falcone 2016.
11. Un elemento che si evince bene dalla consultazione di *Open Data 200 Italia*, il primo e unico studio sistematico compiuto nel nostro Paese sulle imprese italiane che utilizzano i dati aperti nelle loro attività, segnalato anche all'interno del sito governativo italiano *dati.gov.it*. Il progetto è stato sviluppato nel 2016-2017 dal GovLab della New York University in collaborazione con la Fondazione Bruno Kessler di Trento.

La crescita complessiva della conoscenza collettiva che il riutilizzo dei dati aperti garantisce, infatti, accresce la democraticità delle decisioni, non solo indirettamente, grazie alla ricerca scientifica organizzata (Università e Centri di ricerca)[12], ma, più direttamente, grazie alla conoscenza prodotta dai cittadini per l'esercizio dei loro diritti di partecipazione nei processi decisionali pubblici, siano essi normativi o, più diffusamente, amministrativi.

La diffusione e il riutilizzo dei dati in possesso delle amministrazioni permette ai cittadini – o meglio, ai cittadini organizzati[13]– di partecipare attivamente e con una maggiore consapevolezza ai processi decisionali pubblici, fornendo nuove informazioni e nuove conoscenze alle amministrazioni (che non possedevano o non avevano interesse ad elaborare), fino anche a produrre una conoscenza alternativa a quella dei poteri pubblici[14]. Una partecipazione informata e consapevole che rappresenta un importante ritorno conoscitivo per le amministrazioni, le quali acquisiscono nuova conoscenza sulla realtà su cui intervengono, che spesso – per mancanza di tempo, di risorse umane e strumentali o per semplice "cecità" rispetto ad interessi che non erano ancora emersi nel procedimento – non avrebbero potuto acquisire diversamente[15].

Per quanto riguarda il secondo, la maggiore democraticità delle decisioni pubbliche è garantita anche dalla possibilità per i cittadini di controllare, attraverso la conoscenza derivante dai dati aperti, l'operato dei poteri pubblici. La possibilità di accedere, riutilizzare ed elaborare liberamente i dati in merito al funzionamento, all'organizzazione, alle decisioni delle amministrazioni pubbliche permette una valutazione consapevole delle scelte compiute e dei risultati raggiunti dalle stesse, accrescendo la trasparenza delle loro attività. I dati aperti, se correttamente utilizzati, contribuiscono, dunque, anche a rendere la collettività un soggetto informato, capace di controllare democraticamente l'operato delle amministrazioni e di attivare, principalmente con le elezioni, la responsabilità politica degli organi di vertice[16].

12. Il contributo dei risultati della ricerca scientifica (umanistica, sociale o delle c.d. scienze dure) derivante dall'elaborazione e dal riutilizzo dei dati pubblici alla democraticità delle decisioni è evidente – in quanto essa può migliorare in via generale la conoscenza scientifica sui fenomeni sociali, naturali, economici più importanti, proprio perché derivante da un insieme di dati che non erano ancora stati elaborati e interpretati con metodo scientifico. La letteratura sulla conoscenza (e sui dati che ne sono il fondamento) come bene comune e sulla progressiva privatizzazione della conoscenza attraverso i segreti industriali/commerciali è cospicua. Si v. per tutti Ostrom-Hess 2009, oppure, nella letteratura italiana si v. per esempio Caso 2022, Mattei 2020, Resta 2013, Resta 2011. Interessante anche la prospettiva che emerge in Cavallo Perin 2021, in cui l'autore sottolinea come la conoscenza ricavabile dai dati aperti e, più in generale, dalla libera circolazione dei dati, anche in possesso dei privati, deve essere garantita a tutti in quanto costituisce un vero e proprio diritto alla conoscenza, strumentale allo sviluppo dell'identità individuale e collettiva e ha un fondamento costituzionale nella promozione della cultura e del patrimonio culturale (art. 9, Cost.), nel diritto all'informazione e all'identità personale (artt. 21 e 22, Cost.), nella libertà di scienza (art. 33, Cost.), e più in generale nel principio personalista e di solidarietà (art. 2, Cost.).
13. È chiaro come il singolo cittadino non sia quasi mai in grado di ricavare da solo nuova conoscenza dall'accesso e dal riutilizzo dei dati pubblici, ma è evidente come sia necessaria la presenza e il lavoro di organismi intermedi che elaborino la grande mole di dati in formato aperto messa a disposizione delle amministrazioni per produrre nuova conoscenza. In questo senso si v. Ponti 2019.
14. Per un esempio di utilizzo dei dati per produrre una conoscenza alternativa a quella prodotta dalle amministrazioni, si permetta di richiamare Falcone 2017.
15. Sul fondamento costituzionale del legame tra partecipazione alle decisioni pubbliche, in particolare amministrative, e dati aperti si v. per tutti Carloni 2014.
16. Sui numerosi paradigmi della trasparenza e sul ruolo dei dati aperti, intesi come strumento di trasparenza amministrativa, per l'esercizio di un corretto funzionamento democratico si v. Carloni 2022, Carloni 2014, Ponti 2011.

Dunque, oltre alla finalità economica – che pure è parte integrante di questa concezione teorica[17] – è la maggiore democraticità delle decisioni pubbliche – attraverso una partecipazione informata e il controllo democratico sull'operato dei poteri pubblici – che fa rientrare pienamente i dati aperti dentro la teoria dei *commons*[18]. Una finalità che rende il ritorno conoscitivo nella decisione pubblica – derivante, appunto, dal riutilizzo dei dati aperti da parte dei cittadini organizzati – non solo una parte integrante, insieme al libero accesso e al riutilizzo senza condizioni dei dati pubblici, ma una parte fondamentale del paradigma degli open data. Questo aspetto caratterizza profondamente le due finalità democratiche che giustificano lo sganciamento della titolarità dall'accesso al bene, la cui assenza o sottovalutazione potrebbe alterare il senso profondo del paradigma dei dati aperti, rendendoli, di fatto, solo un nuovo e profittevole asset che i soggetti privati possono utilizzare nelle dinamiche di mercato.

Inoltre, è utile precisare una interessante evoluzione del paradigma dei dati aperti. Come abbiamo avuto modo di sottolineare fino ad ora, la filosofia degli open data ha sempre avuto come oggetto i dati in possesso delle amministrazioni, anche se non ha mai escluso che si potesse scindere la titolarità dall'accesso (e dal loro riutilizzo) anche ai dati di interesse pubblico in possesso dei soggetti privati, dunque con lo stesso valore collettivo dei dati pubblici. Una prospettiva che, invece, sta emergendo progressivamente, in particolare nelle riflessioni che valorizzano i dati aperti come un bene "essenziale" da condividere all'interno di una determinata comunità sulla base del principio di solidarietà, dunque, su base volontaristica[19]. Una prospettiva diversa – emersa anche sotto la spinta del legislatore, come vedremo – ma che resta coerente con la teoria dei *commons*, cioè con l'idea del superamento della titolarità pubblica e privata dei beni "essenziali" per la collettività per garantire loro un accesso e un riutilizzo generalizzato.

Queste riflessioni sulle finalità e sugli elementi fondamentali della teoria dei dati aperti, dunque, non possono che essere la base di partenza per valutare come e se queste caratteristiche, in particolare queste finalità, siano state declinate dal legislatore europeo nelle numerose e crescenti norme dedicate alla circolazione e all'"apertura" dei dati, in particolare quelli in possesso delle amministrazioni pubbliche.

3. I dati aperti nelle norme europee: dalla commercializzazione alla diffusione di conoscenza e ritorno

Come è noto, da tempo l'Unione europea ha deciso di utilizzare la propria competenza sul mercato unico (*ex* art. 114 TFUE) per adottare una serie di testi normativi che vanno a disciplinare la circolazione dei dati nell'Unione.

Nel tempo, si è passati da una disciplina settoriale, anche se in alcuni casi di grande rilevanza – come la disciplina sulla protezione dei dati personali[20], quella sulla circolazione dei dati non personali[21] o quella sul riutilizzo dei dati pubblici (nelle sue numerose versioni 2003-2013-2019)[22] – ad una

17. Sulle finalità economiche come parte integrante del paradigma si v. in particolare Purtova–van Maanen 2023, Solda-Kutzman 2011.
18. In particolare, queste due finalità hanno contribuito a costruire il paradigma dell'*open government*, dell'amministrazione aperta, cioè di un'amministrazione partecipata, *accountable* e trasparente. Su questo si v. Galetta 2019, Costantino 2015, Carloni 2014, Bonomo 2012. Un paradigma che, inoltre, ha un solido fondamento di rilievo costituzionale, come si dirà nell'ultimo paragrafo.
19. In questo senso si v. Van Maanen–Ducuing–Fia 2024. Nella letteratura italiana si v., Basunti 2024, Castaldo 2024, Ricci 2024, Resta 2022, Cavallo Perin 2021.
20. Si fa riferimento al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE.
21. Ci si riferisce al Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.
22. Ci riferiamo alle tre direttive europee che nel tempo hanno disciplinato il riutilizzo dei dati pubblici. In ordine, la Direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, relativa al riutilizzo

strategia più generale, esplicitata nella *Strategia europea per i dati*[23], poi attuata attraverso una serie di regolamenti che oggi compongono una disciplina sulla circolazione dei dati nel mercato unico europeo molto corposa[24], che tiene conto del forte sviluppo del mercato digitale degli ultimi decenni.

Un quadro normativo complesso – che qui richiameremo solo rispetto alle disposizioni che riguardano i dati aperti e la loro circolazione tra gli Stati membri – che, allo stesso tempo, è da intendersi come una disciplina minima sulla circolazione dei dati[25]. L'intento dichiarato del legislatore europeo è quello di armonizzare le diverse norme nazionali, senza mettere in discussione né le norme statali sui diritti di accesso ai dati pubblici, né quelle (prevalentemente europee, ma anche di attuazione nazionale) sulla protezione dei dati personali o sulla protezione dei segreti commerciali e industriali.

In ogni caso emerge un quadro normativo che ha progressivamente legato l'"apertura" dei dati soprattutto ad una delle finalità del paradigma degli open data: lo sviluppo economico e la libertà di iniziativa economica, in particolare dopo l'approvazione del Regolamento (UE) 2022/868, il c.d. *Data governance Act* e del Regolamento (UE) 2023/2854, il c.d. *Data Act*.

Una scelta legislativa che emerge bene se si analizzano i tre aspetti fondamentali delle norme dedicate ai dati aperti: le categorie di dati oggetto di riutilizzo e di "apertura"; le situazioni giuridiche soggettive che vengono individuati per assicurare che i dati vengano effettivamente aperti; le finalità cui questa disciplina è preposta.

In via preliminare, però, è utile sottolineare come, nella disciplina europea non è presente una definizione precisa di dati aperti[26], ma, qualora volessimo trovare qualche riferimento, bisognerebbe fare riferimento alle discipline nazionali. In Italia, in particolare, è l'articolo 1, comma 1, lettera l-*ter*) del d.lgs. 7 marzo 2005, n. 82, il c.d. Codice dell'amministrazione digitale (da ora CAD), che contiene una definizione giuridicamente utile di dati aperti.

Il CAD definisce i dati aperti come "i dati che presentano le seguenti caratteristiche: 1) sono disponibili secondo i termini di una licenza o di una previsione normativa che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato; 2) sono accessibili attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, in formati aperti […][27], sono adatti all'utilizzo automatico da parte

dell'informazione del settore pubblico; la Direttiva 2013/37/UE che modifica la direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico; infine, la Direttiva 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico.

23. La strategia è contenuta nella Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Una strategia europea per i dati*, COM (2020) 66 final.

24. Si pensi in particolare al *Data governcance Act*, cioè al 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 e al *Data Act*, il 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.

25. Sulla scelta, molto spesso sbagliata, dell'atto normativo più adatto per disciplinare questa materia si v. Burelli 2025, la quale sottolinea, tra le altre cose, come sta emergendo la tendenza ad usare regolamenti che necessitano un'attuazione nazionale in luogo delle tradizionali direttive. Sulla stessa tendenza, ma relativamente ai dati personali si v. Ponti 2023. Per una riflessione sul cambiamento che questo quadro normativo comporta si v. Pathak 2024, Morace Pinelli 2024, Casolari–Buttaboni–Floridi 2023.

26. A livello europeo è possibile ricavare una definizione simile nell'art. 2, comma 1, punto 13) della direttiva 2019/1024, la quale, riprendendo una definizione già presente nella direttiva 2003/98/CE, parla di "formato leggibile meccanicamente". Sulla definizione di dato aperto si v. Carullo 2025.

27. Riprendendo la definizione presente nell'articolo 1, comma 1, lettera l-*bis*) del CAD, per formato aperto si intende "un formato di dati reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi".

di programmi per elaboratori e sono provvisti dei relativi metadati; 3) sono resi disponibili gratuitamente attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, oppure sono resi disponibili ai costi marginali sostenuti per la loro riproduzione e divulgazione salvo quanto previsto dall'articolo 7 del decreto legislativo 24 gennaio 2006, n. 36"[28].

Una definizione di natura tecnico-operativa, che nel complesso, garantendo la disponibilità e l'accessibilità, permette operativamente il riutilizzo dei dati in possesso delle amministrazioni, anche in modo coerente rispetto alla filosofia degli open data (cioè senza restrizioni nelle finalità e gratuitamente). In via generale, però, evidentemente, questa definizione non è ispirata dalle numerose idealità sottese alla filosofia dei dati aperti, così come la abbiamo descritta nel paragrafo precedente e non la funzionalizza al raggiungimento di specifiche finalità.

3.1. La progressiva espansione delle tipologie di dati oggetto di riutilizzo e di "apertura"

Come abbiamo anticipato, le norme europee hanno, in primo luogo, esteso progressivamente le tipologie di dati oggetto di riutilizzo e di "apertura".

In termini generali, si è passati da una logica documentale, contenuta nella direttiva 2003/98/CE (la c.d. direttiva PSI), in cui l'oggetto del riutilizzo erano solo i documenti in possesso delle amministrazioni pubbliche, ad una logica ibrida e trasversale – introdotta con la direttiva 2013/37/UE e poi confermata dalla direttiva (UE) 2019/1024, dal Regolamento (UE) 2022/868 e dal Regolamento (UE) 2023/2854. Una logica ibrida perché, per quanto riguarda le amministrazioni pubbliche, l'oggetto del riutilizzo rimangono formalmente i documenti, ma in una logica dei dati, in quanto spesso il testo normativo fa riferimento – esplicitamente o in via sostanziale – ai dati in possesso delle amministrazioni. Inoltre, è anche una logica trasversale visto che, con i due regolamenti appena richiamati, alcune forme di riutilizzo cominciano ad essere applicate anche ai dati in possesso dei soggetti privati[29].

La direttiva (UE) 2019/1024, in particolare, ha esteso l'applicazione del regime di accesso e riutilizzo ai documenti e ai dati in possesso di tutti gli enti pubblici degli Stati membri, delle imprese pubbliche, degli organismi di diritto pubblico e dei privati che erogano servizi di interesse generale[30]. Oltre a questa categoria principale di documenti e dati, cioè in possesso di questi enti, la direttiva ha esteso il regime di "apertura" anche a tre categorie specifiche di dati di particolare valore collettivo.

In primo luogo ai dati dinamici, definiti come i "documenti in formato digitale, soggetti ad aggiornamenti frequenti o in tempo reale, in particolare a causa della loro volatilità o rapida obsolescenza"[31]. Facciamo riferimento ai c.d. *big data*, cioè a tutti quei dati – in questo caso omogenei, ma spesso anche molto eterogenei tra loro – che vengono prodotti in tempo reale, generalmente da sensori o da tecnologie riconducibili alla galassia dell'*Internet of things* (IoT)[32].

28. Il comma 2 dell'art. 7 in questione, infatti, prevede che il regime di gratuità del dato (o del costo marginale di riproduzione del documenti che lo contiene) previsto nel comma 1 "non trova applicazione per: a) le biblioteche, comprese quelle universitarie, i musei e gli archivi; b) le pubbliche amministrazioni e gli organismi di diritto pubblico che devono generare utili per coprire una parte sostanziale dei costi inerenti allo svolgimento dei propri compiti di servizio pubblico; c) le imprese pubbliche".
29. Una logica che è ben visibile leggendo il testo della direttiva (UE) 2019/1024, per quanto riguarda le amministrazioni, e le disposizioni del *Data governance Act* e del *Data Act*, per quanto riguarda i soggetti privati. Sul fondamentale passaggio dalla logica dei documenti alla logica dei dati nella disciplina del riutilizzo, avvenuto molto più chiaramente nella disciplina italiana, in particolare dopo il d.lgs. 14 marzo 2013, n. 33, si v. Falcone 2016, Ponti 2008.
30. Si v. l'art. 1, comma 1 della direttiva (UE) 2019/1024.
31. Si v. l'art. 2, comma 1, punto 8) della direttiva (UE) 2019/1024.
32. Sui *big data*, sui loro caratteri e sul loro valore conoscitivo si permetta di rimandare a Falcone 2023 e Falcone 2017. Più di recente si v. anche Mazzei 2023, la quale contestualizza il fenomeno dei *big data* al contesto normativo più recente.

In secondo luogo, ai dati della ricerca, definiti come i "documenti in formato digitale, diversi dalle pubblicazioni scientifiche, raccolti o prodotti nel corso della ricerca scientifica e utilizzati come elementi di prova nel processo di ricerca, o comunemente accettati nella comunità di ricerca come necessari per convalidare le conclusioni e i risultati della ricerca"[33].

Infine, alle c.d. serie di dati di elevato valore, cioè quei "documenti il cui riutilizzo è associato a importanti benefici per la società, l'ambiente e l'economia, in particolare in considerazione della loro idoneità per la creazione di servizi, applicazioni a valore aggiunto e nuovi posti di lavoro dignitosi e di alta qualità, nonché del numero dei potenziali beneficiari dei servizi e delle applicazioni a valore aggiunto basati su tali serie di dati"[34]. Questi ultimi sono considerati dati di particolare interesse pubblico, per il quale l'ordinamento europeo ha previsto, come si dirà più avanti, una sorta di potere di coordinamento in capo alla Commissione europea simile a quello presente nella nostra Costituzione, in particolare nell'art. 117, comma 2, lett. r)[35].

Oltre ai dati previsti direttamente dalla direttiva del 2019, forme di "apertura" e di circolazione si applicano anche ad altre tipologie di dati, contenute in altri testi normativi.

Il Regolamento (UE) 2018/1807, per esempio, garantisce la libera circolazione anche ai dati non personali, definiti come "insiemi di dati aggregati e anonimizzati usati per l'analisi dei megadati, i dati sull'agricoltura di precisione che possono contribuire a monitorare e ottimizzare l'uso di pesticidi e acqua, o i dati sulle esigenze di manutenzione delle macchine industriali"[36].

Il Regolamento (UE) 2022/868, cioè il *Data governance Act*, invece – con l'intento di estendere ulteriormente le categorie di dati in possesso delle amministrazioni da rendere liberamente accessibili e riutilizzabili – ha previsto un regime di riutilizzo specifico per "i dati detenuti da enti pubblici, che sono protetti per motivi di: a) riservatezza commerciale, compresi i segreti commerciali, professionali o d'impresa; b) riservatezza statistica; c) protezione dei diritti di proprietà intellettuale di terzi; o d) protezione dei dati personali, nella misura in cui tali dati non rientrano nell'ambito di applicazione della direttiva (UE) 2019/1024"[37].

Infine, le norme europee hanno introdotto, per la prima volta, la possibilità di riutilizzare i dati di interesse pubblico detenuti da imprese private.

33. Si v. l'art. 2, comma 1, punto 9) della direttiva (UE) 2019/1024. Il Considerando 27 della direttiva specifica che "sono dati della ricerca per esempio le statistiche, i risultati di esperimenti, le misurazioni, le osservazioni risultanti dall'indagine sul campo, i risultati di indagini, le immagini e le registrazioni di interviste, oltre a metadati, specifiche e altri oggetti digitali".
34. Si v. l'art. 2, comma 1, punto 10) della direttiva (UE) 2019/1024. Il Considerando 66 della direttiva fa riferimento, solo in modo esemplificativo, a dati come "i codici di avviamento postale, le mappe e le carte nazionali e locali (dati geospaziali), il consumo energetico e le immagini satellitari (dati relativi all'osservazione della terra e all'ambiente), i dati in situ provenienti da strumenti e previsioni meteorologiche (dati meteorologici), gli indicatori demografici e economici (dati statistici), i registri delle imprese e gli identificativi di registrazione (dati relativi alle imprese e alla proprietà delle imprese), la segnaletica stradale e le vie navigabili interne (dati relativi alla mobilità)".
35. Sull'introduzione di un potere di coordinamento dei dati europeo si permetta di rimandare a Falcone 2023. In generale, sul potere di coordinamento derivante dall'art. 117, comma 2, lett. r) si v. Alberti 2022, Merloni 2008, Ponti 2008, Marongiu 2005.
36. Troviamo questo riferimento nel Considerando 9 del Regolamento (UE) 2018/1807.
37. Si v. l'art. 3, comma 1, del Regolamento (UE) 2022/868. A differenza della direttiva (UE) 2019/1024, però, l'art. 3, comma 2, esclude i dati detenuti: dalle imprese pubbliche; dalle emittenti di servizio pubblico o dalle società o organismi collegati per l'adempimento di un compito di radiodiffusione di servizio pubblico; dagli enti culturali e di istruzione; da tutti gli enti pubblici se i dati sono protetti per motivi di pubblica sicurezza, difesa o sicurezza nazionale. Vengono esclusi anche i dati la cui fornitura è un'attività che esula dall'ambito dei compiti di servizio pubblico degli enti pubblici.

In via generale, con le disposizioni del Regolamento (UE) 2023/2854, cioè del *Data Act*, il quale prevede che "un ente pubblico, la Commissione, la Banca centrale europea o un organismo dell'Unione" possano richiedere l'accesso e l'utilizzo di "taluni dati, ivi compresi i pertinenti metadati necessari per interpretare e utilizzare tali dati, per svolgere le proprie funzioni statutarie nell'interesse pubblico" in possesso di imprese private[38].

In via più specifica, invece, con alcune previsioni del c.d. *Digital Services Act*, che permettono il riutilizzo dei dati relativi alle attività di moderazione dei contenuti presenti nelle relazioni annuali che le grandi piattaforme devono stilare ogni anno e presentare alla Commissione. Secondo l'art. 55, comma 1, del Regolamento (UE) 2022/2065, "i coordinatori dei servizi digitali elaborano relazioni annuali sulle attività da essi svolte a norma del presente regolamento, compreso il numero di reclami ricevuti a norma dell'articolo 53 e una panoramica del loro seguito" e "rendono le relazioni annuali disponibili al pubblico in un formato leggibile meccanicamente, fatte salve le norme applicabili in materia di riservatezza delle informazioni a norma dell'articolo 84"[39].

Rispetto alla direttiva del 2003 e alle norme nazionali – come quella italiana, la quale prevedeva già un diritto al riutilizzo molto più esteso della direttiva stessa[40] – dunque, c'è stata una enorme crescita delle categorie di dati oggetto di forme di "apertura". Una crescita progressiva – ed è questo l'elemento realmente innovativo – che ha legato in modo sempre più evidente la necessità di "aprire" le banche dati (e di permettere il riutilizzo dei dati) con il valore conoscitivo collettivo che quei dati possono generare e, dunque, con la loro rilevanza pubblica: basti pensare, in modo particolare, alle c.d. serie di dati di elevato valore, che abbiamo richiamato o, ancora, alla possibilità, garantita dal *Data Act*, di riutilizzare i dati in possesso dei soggetti privati utili per l'esercizio di compiti di interesse pubblico.

Le norme europee sui dati, dunque, hanno reso effettivo quel riferimento – spesso presente nei documenti della Commissione[41] – al concetto di "dati per il bene pubblico"[42]. Una categoria di dati di interesse pubblico – da intendersi in senso lato del termine, cioè non legato per forza all'esercizio di funzioni pubbliche, ma piuttosto al valore conoscitivo che possono in potenza generare – dunque, costituita da un insieme di dati, diversi tra di loro, in possesso sia di soggetti pubblici, sia di soggetti privati, che giustifica l'intervento normativo teso a favorire (e qualche volta ad obbligare) l'"apertura"

38. Si v. l'art. 14 del Regolamento (UE) 2023/2854.

39. L'art. 55, comma 2, specifica che "La relazione annuale comprende inoltre le informazioni seguenti: a) il numero e l'oggetto degli ordini di contrastare contenuti illegali e degli ordini di fornire informazioni emessi in conformità degli articoli 9 e 10 da qualsiasi autorità giudiziaria o amministrativa nazionale dello Stato membro del coordinatore dei servizi digitali interessato; b) il seguito dato a tali ordini, quale comunicato al coordinatore dei servizi digitali ai sensi degli articoli 9 e 10".

40. Per un approfondimento su questo punto di permetta di richiamare Falcone 2016 e i contributi presenti in Ponti 2016.

41. Un concetto, come abbiamo segnalato all'inizio di questo lavoro, già presente nella Comunicazione della Commissione, *Costruire un'economia dei dati europea*, COM/2017/9 final e nella Commission Staff, *Working Document on the free flow of data and emerging issues of the European data economy*, SWD (2017) 2 final, ma in particolare nella nota Comunicazione Una strategia europea per i dati, COM/2020/66 final.

42. Si v. p. 7 della Comunicazione *Una strategia europea per i dati*, COM/2020/66 final in cui si definiscono come quei dati "creati dalla società e [che] possono essere utili per far fronte ad emergenze quali inondazioni e incendi, per consentire alle persone di vivere più sane e più a lungo, per migliorare i servizi pubblici, per contrastare il degrado ambientale e i cambiamenti climatici e, se necessario e proporzionato, per garantire una lotta più efficiente alla criminalità. I dati generati dal settore pubblico, al pari del valore creato, dovrebbero essere messi a disposizione per il bene pubblico garantendone, anche tramite un accesso preferenziale, l'utilizzo da parte di ricercatori, altre istituzioni pubbliche, PMI o start-up. Anche i dati provenienti dal settore privato possono offrire un contributo significativo se utilizzati come beni pubblici. L'uso di dati aggregati e anonimizzati dei social media può ad esempio costituire un mezzo efficace per integrare i referti dei medici di base in caso di epidemia".

e la diffusione di una determinata categoria di dati da parte dei soggetti pubblici e privati.

Da questo punto di vista, l'impianto normativo europeo – se lo si guarda rispetto alla crescita delle forme di accesso e di riutilizzo che hanno permesso l'emersione di una categoria generale di dati di interesse pubblico – è molto coerente con la logica dei dati come *commons*.

È interessante allora provare a comprendere fin dove si spinga questa coerenza, in particolare, è necessario comprendere in che modo viene assicurato lo sganciamento tra titolarità dei dati di interesse pubblico e accesso e riutilizzo degli stessi e per quale motivo questi ultimi vengono consentiti: elementi che, come abbiamo sottolineato in precedenza, stanno alla base del regime giuridico dei *commons*. Per farlo è utile ricostruire quali sono le situazioni soggettive, gli obblighi e soprattutto gli elementi di doverosità più importanti a garanzia dell'accesso e del riutilizzo dei dati di interesse pubblico previsti nel pacchetto di norme europee in analisi.

3.2. Gli obblighi (i conseguenti diritti) e le doverosità a garanzia dell'accesso, del riutilizzo e della libera circolazione dei dati in possesso delle amministrazioni e dei soggetti pubblici

In prima battuta è utile precisare che questo tipo di disposizioni sono state affiancate da importanti disposizioni di "infrastruttura", cioè da disposizioni che mirano a garantire in via generale una cornice normativa che strutturalmente favorisca la circolazione dei dati nel territorio dell'Unione europea.

Facciamo riferimento, da un lato, al divieto per tutti gli Stati membri di prevedere obblighi di localizzazione dei dati non personali, presente nell'art. 4 del Regolamento (UE) 2018/1807. Una disposizione che presenza delle eccezioni[43], ma che – se letta insieme alle previsioni del Regolamento (Ue) 2016/679 sulla protezione e sulla circolazione dei dati personali – garantisce un insieme di norme che favoriscono la circolazione sia dei dati non personali, sia dei dati personali all'interno del mercato unico europeo[44].

Dall'altro lato, si pensi ai diritti di portabilità dei propri dati garantiti ai cittadini e agli utenti, presenti variamente nelle norme che abbiamo richiamato[45].

In primo luogo al diritto alla portabilità previsto dall'articolo 20 del Regolamento (Ue) 2016/679 sulla protezione dei dati personali, che consente all'interessato di ricevere "i dati personali forniti a un titolare, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di trasmetterli a un altro titolare del trattamento senza impedimenti". Un diritto che il Regolamento (UE) 2023/2854 ha esteso a tutti i dati generati da prodotti e servizi connessi (es. IoT, servizi cloud), garantendo agli utenti (consumatori e imprese) il diritto di accedere a questi dati e trasferirli facilmente a un altro fornitore in formati interoperabili (API, standard)[46].

Specularmente anche il Regolamento (UE) 2018/1807 sui dati non personali, all'art. 6 presenta disposizioni che vanno in questo senso: alla Commissione è affidato il compito di incoraggiare e facilitare l'elaborazione di codici di autoregolamentazione a livello dell'Unione, per migliorare la circolazione dei dati non personali, in particolare attraverso la diffusione delle migliori prassi, e per favorire la portabilità dei dati.

Oltre a queste disposizioni di infrastruttura normativa – che favoriscono un quadro generale di circolazione dei dati – sia la direttiva (UE) 2019/1024, in via generale, sia il Regolamento (UE) 2022/868 sulla governance dei dati, in via più specifica, contengono obblighi e doveri di ostensione dei documenti e dei dati in capo ai soggetti pubblici.

L'art. 3 della direttiva (UE) 2019/1024, innanzitutto, introduce l'obbligo in capo alle amministrazioni, alle imprese pubbliche e agli organismi di

43. Secondo il primo comma dell'art. 4 del Regolamento, "gli obblighi di localizzazione di dati sono vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità".
44. Per un quadro di insieme sulle implicazioni derivanti da queste norme sulla circolazione dei dati non personali, dei dati personali e soprattutto dei dati misti, che rappresentano spesso una parte rilevante delle banche dati pubbliche e private si v. Ruggieri 2023, Torregiani 2020.
45. Per una disamina più approfondita sui vari diritti di portabilità si v. Gatti 2023.
46. In questo senso va l'art. 5 del *Data Act*, dedicato al "diritto dell'utente di condividere i dati con terzi".

diritto pubblico di permettere l'accesso e il riutilizzo dei documenti e dei dati in loro possesso.

Secondo l'art. 5 della direttiva questi ultimi devono essere riutilizzabili e messi a disposizione in formati aperti, leggibili meccanicamente, accessibili, reperibili e riutilizzabili, insieme ai rispettivi metadati, sostanzialmente nel rispetto dei principi di *open by default* e *by design*[47]. Il riutilizzo è di regola gratuito per l'utilizzatore[48], ad eccezione di alcuni soggetti pubblici[49], che possono prevedere specifiche tariffe, stabilite con criteri oggettivi, trasparenti e verificabili, in ogni caso non superiore ai costi marginali di riproduzione e manipolazione, maggiorati di un utile ragionevole. Inoltre, l'art. 8 della direttiva prevede che il riutilizzo non è soggetto a condizioni, a meno che non siano giustificate da un obiettivo di interesse pubblico. In ogni caso devono essere sempre obiettive, proporzionate, non discriminatorie e che non riducano la portata del riutilizzo. Infine, sono vietati accordi di esclusiva tra enti pubblici e imprese private, a meno che non siano necessari per l'erogazione di servizi pubblici: in ogni caso devono essere fondati e soggetti a revisione triennale[50].

Come abbiamo già accennato, un regime specifico è previsto per le c.d. serie di dati di elevato valore. L'art. 14 della direttiva prevede che la Commissione europea – utilizzando una sorta di potere di coordinamento dei dati sulla falsariga di quello presente nell'art. 117, comma 2, lett. r) – possa stabilire un elenco di specifiche serie di dati di elevato valore corrispondenti alle categorie di cui all'allegato I, attraverso l'adozione di atti di esecuzione[51]. In ogni caso questi dati devono essere in via generale: disponibili gratuitamente; leggibili meccanicamente; fornite mediante API e, se del caso, anche fornite come download in blocco. Gli atti di esecuzione possono, di fatto, solo specificare le modalità di pubblicazione, che devono essere compatibili con le licenze aperte standard, e le modalità di riutilizzo, che possono includere le condizioni applicabili al riutilizzo, i formati dei dati e dei metadati e le modalità tecniche di diffusione.

È un potere di coordinamento di natura tecnica e vincolata, dunque, che rappresenta una importante evoluzione dei poteri della Commissione in materia di dati. Quest'ultima ha già utilizzato questa facoltà adottando il Regolamento di esecuzione (UE) 2023/138, con il quale ha specificato nel dettaglio le serie di dati di elevato valore, le metodologie di riutilizzo e un metodo di individuazione di tali serie che tiene conto dei desiderata degli Stati membri e delle necessità del mercato[52].

Diverso è il regime del riutilizzo dei documenti e dei dati soggetti ad un regime di riservatezza personale, statistica o commerciale in possesso delle amministrazioni previsto dal Regolamento (UE) 2022/868 sulla governance dei dati. In questo caso

47. Bisogna ricordare che lo stesso art. 5, comma 3, prevede che questi principi, di carattere organizzativo, non introducono "l'obbligo di adeguare i documenti o di crearne per conformarsi a tale paragrafo, né l'obbligo di fornire estratti di documenti, se ciò comporta difficoltà sproporzionate, che vanno al di là della semplice manipolazione", così come non obbligano i soggetti pubblici "di continuare a produrre e a conservare un certo tipo di documento per permetterne il riutilizzo da parte di un'organizzazione del settore privato o pubblico".
48. Si v. l'art. 6 della direttiva (UE) 2019/1024. Lo stesso articolo concede la possibilità di fare pagare il costo marginale dell'operazione di riproduzione oppure, se è il caso, il costo di anonimizzazione, al fine di proteggere i dati personali. Tranne che per le serie di dati di elevato valore pubblico delle imprese pubbliche e delle biblioteche/archivi/musei e dei dati della ricerca.
49. Le imprese pubbliche, le biblioteche, i musei, gli archivi e le amministrazioni che devono generare proventi per coprire i costi di erogazione di compiti di servizio pubblico non sono soggette a questo regime.
50. Si v. l'art. 12 della direttiva (UE) 2019/1024.
51. Ricordiamo che l'allegato I della direttiva (UE) 2019/1024 fa riferimento alle seguenti categorie: dati geospaziali; dati relativi all'osservazione della terra e all'ambiente; dati meteorologici; dati statistici; dati relativi alle imprese e alla proprietà delle imprese; dati relativi alla mobilità.
52. Il Regolamento di esecuzione (UE) 2023/138 della Commissione del 21 dicembre 2022 che stabilisce un elenco di specifiche serie di dati di elevato valore e le relative modalità di pubblicazione e riutilizzo contiene, infatti, numerose eccezioni e modalità di riutilizzo mitigate o alternative proprio per bilanciare la necessità di diffondere il più possibile questo tipo di dati con la volontà degli Stati membri.

non abbiamo un dovere di ostensione in capo alle amministrazioni, ma soltanto la facoltà di prevedere o meno l'accesso e il riutilizzo di questo tipo di dati, seguendo, in caso affermativo, le specifiche modalità di apertura e di riutilizzo contenute nel regolamento.

È chiaro, però, come questa facoltà – essendo fortemente promossa dal legislatore europeo al fine di garantire la maggiore circolazione possibile dei dati in possesso delle amministrazioni – possa essere interpretata come una forma di doverosità in capo alle amministrazioni[53]. Questo elemento lo si evince sia leggendo l'art. 5, comma 1 del Regolamento – in cui si afferma che "gli Stati membri garantiscono che gli enti pubblici siano dotati delle necessarie risorse per conformarsi al presente articolo" – sia il comma 6 dello stesso articolo – che affida alle amministrazioni comunque un ruolo di soccorso attivo a favore dei potenziali riutilizzatori, anche con l'aiuto degli organismi competenti di cui all'art. 7[54].

Più precisamente, secondo l'art. 5 del regolamento, le amministrazioni che intendono concedere l'accesso e il riutilizzo di una delle categorie summenzionate devono predisporre una procedura di richiesta del riutilizzo attraverso uno sportello unico[55]. Le amministrazioni possono essere anche assistite dagli organismi competenti per la predisposizione delle procedure e delle misure organizzative necessarie[56].

In caso di accoglimento della richiesta, le amministrazioni devono comunque adottare misure che, nel permettere il riutilizzo dei dati richiesti, salvaguardino la riservatezza personale o quella commerciale/industriale, attraverso specifiche misure tecniche e organizzative, anche predisponendo ambienti adeguati per permettere l'effettivo accesso e riutilizzo di questi dati[57]. In ogni caso, le

53. Per un approfondimento sul concetto di doverosità resta essenziale Goggiamani 2005.

54. Il comma 6 afferma che "qualora il riutilizzo dei dati non possa essere consentito in conformità degli obblighi di cui ai paragrafi 3 e 4 del presente articolo e non vi sia alcuna base giuridica per la trasmissione dei dati a norma del regolamento (UE) 2016/679, l'ente pubblico si adopera al meglio, conformemente al diritto dell'Unione e nazionale, per fornire assistenza ai potenziali riutilizzatori nel richiedere il consenso degli interessati o l'autorizzazione dei titolari dei dati i cui diritti e interessi possono essere interessati da tale riutilizzo, ove ciò sia fattibile senza un onere sproporzionato per l'ente pubblico. Qualora fornisca tale assistenza, l'ente pubblico può essere assistito dagli organismi competenti di cui all'articolo 7, paragrafo 1".

55. Secondo l'art. 8 del regolamento "gli Stati membri istituiscono un nuovo ente o designano un ente o una struttura esistente quale sportello unico. Lo sportello unico può essere collegato a sportelli settoriali, regionali o locali. Le funzioni dello sportello unico possono essere automatizzate a condizione che l'ente pubblico garantisca un sostegno adeguato".

56. Secondo l'art. 7 del regolamento "Ai fini della realizzazione dei compiti di cui al presente articolo, ciascuno Stato membro designa uno o più organismi competenti, che possono essere competenti per specifici settori, per assistere gli enti pubblici che concedono o rifiutano l'accesso al riutilizzo delle categorie di dati di cui all'articolo 3, paragrafo 1. Gli Stati membri possono istituire uno o più organismi competenti nuovi o avvalersi di enti pubblici esistenti o di servizi interni di enti pubblici che soddisfano le condizioni stabilite dal presente regolamento". Il d.lgs. 7 ottobre 2024 n. 144 ha individuato l'Agenzia per l'Italia digitale (AgID) come organismo competente, la quale dovrà collaborare, a seconda delle finalità del caso, sia con il Garante per la protezione dei dati personali, l'Agenzia per la cybersicurezza nazionale (ACN) e l'Autorità Garante della Concorrenza e del Mercato (AGCM).

57. In particolare l'art. 5 paragrafo 3 del regolamento sulla governance dei dati prevede che "Gli enti pubblici garantiscono, conformemente al diritto dell'Unione e nazionale, la tutela della natura protetta dei dati. Essi garantiscono il rispetto dei requisiti seguenti: a) concedere l'accesso per il riutilizzo dei dati soltanto qualora l'ente pubblico o l'organismo competente abbia garantito, in seguito alla richiesta di riutilizzo, che i dati sono stati: i) anonimizzati, nel caso di dati personali; e ii) modificati, aggregati o trattati mediante qualsiasi altro metodo di controllo della divulgazione, nel caso di informazioni commerciali riservate, compresi i segreti commerciali o i contenuti protetti da diritti di proprietà intellettuale; b) accedere ai dati e riutilizzare gli stessi da remoto all'interno di un ambiente di trattamento sicuro, fornito o controllato dall'ente pubblico; c) accedere ai dati e riutilizzare gli stessi all'interno dei locali fisici in cui si trova l'ambiente di trattamento sicuro,

amministrazioni possono anche riservarsi il diritto di verificare il processo, i mezzi e i risultati del trattamento dei dati effettuato dal riutilizzatore, anche vietando l'uso dei risultati, al fine di tutelare l'integrità della protezione dei dati e i diritti e gli interessi commerciali ed intellettuali dei terzi[58].

A protezione di questi diritti e interessi, il regolamento prevede anche un obbligo di riservatezza – che vieta la divulgazione di qualsiasi informazione che comprometta i diritti e gli interessi di terzi e che il riutilizzatore possa aver acquisito malgrado le misure di tutela adottate – e un divieto generalizzato di reidentificare gli interessati cui si riferiscono i dati in capo ai riutilizzatori[59].

Nel caso in cui l'amministrazione decida di fare accedere e riutilizzare una o più categorie di dati protetti, a differenza delle previsioni generali, l'art. 6 del regolamento prevede che esse possano imporre delle tariffe, le quali devono sempre essere trasparenti, non discriminatorie, proporzionate e oggettivamente giustificate e non devono limitare la concorrenza.

Inoltre, il comma 4 dell'art. 6 del regolamento prevede la possibilità per le amministrazioni e gli enti pubblici di applicare tariffe ridotte o nulle per incentivare il riutilizzo di queste specifiche categorie di dati a fini non commerciali, ad esempio per la ricerca scientifica o da parte delle PMI e delle start-up, in conformità delle norme sugli aiuti di Stato. A questo fine, la disposizione prevede anche la possibilità di formare un elenco di categorie di riutilizzatori a cui i dati sono forniti a una tariffa ridotta o a titolo gratuito.

Anche l'art. 4 del regolamento sulla governance dei dati – come l'art. 12 della direttiva del 2019 – vieta gli accordi o pratiche che concedono diritti esclusivi a determinati soggetti (pubblici o privati) o che in qualsiasi modo limitano la disponibilità di dati per il riutilizzo da parte dei soggetti non coinvolti negli accordi. L'unica eccezione è prevista nel caso in cui il diritto esclusivo sia necessario alla fornitura di un servizio o di un prodotto di interesse generale, senza il quale non sarebbe altrimenti possibile. In questo caso il diritto di esclusiva può essere concesso nel rispetto dei principi di trasparenza, parità di trattamento e non discriminazione e, in ogni caso non può superare i 12 mesi.

Il regime di "apertura" dei dati oggetto di riservatezza privata (di natura personale o commerciale) o statistica, previsto nel regolamento sulla governance dei dati, dunque, si allontana dal modello generale previsto dalla direttiva (UE) 2019/1024: si passa dalla obbligatorietà alla facoltà/doverosità; da un preciso regime di accesso e di riutilizzo, sostanzialmente gratuito e libero, ad un regime di accesso e di riutilizzo condizionato, non solo dalla volontà dei soggetti pubblici a consentirlo, ma in particolare dalla predisposizione di misure procedurali e organizzative, obblighi di riservatezza e divieti di pubblicazione dei risultati del riutilizzo a tutela delle varie forme di riservatezza privata.

A ben vedere, l'elemento maggiormente critico non è tanto l'introduzione di condizionalità al libero accesso e riutilizzo dei dati aperti, ma alle finalità sottese a queste condizioni, le quali, infatti, vengono introdotte solo al fine di garantire altri diritti e interessi privati – che meritano senz'altro forme di protezione – e non anche per assicurare pienamente la realizzazione di tutte le finalità legate alla filosofia dei dati aperti.

I due diversi regimi di "apertura" dei dati in possesso delle amministrazioni, dunque, prevedono una separazione tra titolarità e accessibilità/riutilizzo non sempre coerente con la logica dei dati aperti, che abbiamo analizzato all'inizio di questo lavoro: il regime contenuto nella direttiva (UE) 2019/1024 è più in linea con l'idea sottesa alla filosofia degli open data, fondata sull'accesso libero e gratuito e sul riutilizzo senza condizioni, nonostante qualche differenziazione legata ad alcuni dati in possesso di specifici soggetti pubblici (imprese pubbliche, biblioteche, musei, archivi e le amministrazioni che erogano servizi pubblici); mentre quello contenuto nel Regolamento (UE) 2022/868 è lontano dalla filosofia dei dati aperti, frenato da un approccio eccessivamente garantista, non tanto verso la protezione dei dati personali (che resta strumentale alla protezione di un diritto

rispettando rigorose norme di sicurezza, a condizione che l'accesso remoto non possa essere consentito senza compromettere i diritti e gli interessi di terzi".

58. Si v. il comma 4 dell'art. 5 del Regolamento (UE) 2022/868.

59. Si v. il comma 5 dell'art. 5 del Regolamento (UE) 2022/868.

fondamentale come la riservatezza delle persone), ma verso i segreti commerciali ed industriali.

3.3. I diritti e gli obblighi a garanzia dell'accesso, del riutilizzo dei dati in possesso dei soggetti privati

Il vero elemento innovativo della disciplina sui dati aperti è l'introduzione da parte del Capo V del Regolamento (UE) 2023/2854 del nuovo regime del riutilizzo dei dati in possesso dei soggetti privati. Un regime molto diverso rispetto a quello applicabile ai dati in possesso delle amministrazioni pubbliche, ma che prevede, per la prima volta, un regime di accesso e riutilizzo condizionato – nel tempo e nella portata – e diversificato – a seconda della dimensione delle imprese – ai dati in possesso dei privati.

L'art. 14 del Regolamento prevede, in via generale, che le amministrazioni pubbliche e gli enti pubblici, compresa la Commissione, la Banca centrale europea o un organismo dell'Unione, possano richiedere motivatamente alle imprese di qualsiasi dimensione (cioè ai c.d. titolari dei dati) l'accesso a taluni dati in loro possesso, ivi compresi i relativi metadati necessari per interpretarli e utilizzarli correttamente, "per svolgere le proprie funzioni statutarie nell'interesse pubblico"[60].

I dati possono essere richiesti, secondo l'art. 15 del regolamento, solo a determinate condizioni, che si differenziano, appunto, nella portata e rispetto ai soggetti a cui è possibile richiedere i dati. Innanzitutto è possibile richiedere l'accesso e il riutilizzo dei dati privati per necessità eccezionali, cioè "se i dati sono necessari per rispondere a un'emergenza pubblica e l'ente pubblico non può ottenere tali dati con mezzi alternativi in modo tempestivo ed efficace a condizioni equivalenti".

In secondo luogo è possibile farlo nei casi in cui le amministrazioni e gli enti pubblici si trovino in oggettiva difficoltà nel reperire in modo alternativo quei dati per l'esercizio delle loro funzioni. L'art. 15 del regolamento specifica che quando un'amministrazione o un ente pubblico "abbia individuato dati specifici la cui mancanza gli impedisce di svolgere un compito specifico svolto nell'interesse pubblico esplicitamente previsto dalla legge, quali la redazione di statistiche ufficiali, la mitigazione o la ripresa dopo un'emergenza pubblica" oppure "abbia esaurito tutti gli altri mezzi a sua disposizione per ottenere tali dati, compresi, l'acquisto dei dati sul mercato ai prezzi di mercato o il ricorso a obblighi vigenti in materia di messa a disposizione dei dati oppure l'adozione di nuove misure legislative che potrebbero garantire la tempestiva disponibilità dei dati"[61], può richiedere, motivandone le ragioni, l'accesso e il riutilizzo a quei dati, ma solo alle imprese di grandi e medie dimensioni (ma non anche alle micro e piccole imprese) e solo relativamente ai dati non personali in loro possesso.

La richiesta dei soggetti pubblici deve essere corredata da una serie di informazioni relativi ai dati richiesti; alle procedure di trattamento, di condivisione con terzi e di conservazione che si intende mettere in atto; alle finalità per le quali si vogliono utilizzare i dati: tutte le informazioni necessarie per permettere alle imprese di valutare la richiesta delle amministrazioni[62].

In via generale, secondo l'art. 18 del regolamento, il titolare dei dati che riceve la richiesta mette a disposizione i dati "senza indebito ritardo, tenendo conto delle misure tecniche, organizzative e giuridiche necessarie"[63]. Però, lo stesso art. 18, dà la possibilità al soggetto privato di rifiutare la richiesta o di chiederne la modifica. In questo ultimo caso, considerando la condizione di urgenza o di grave necessità che di fatto autorizzano questi accessi, il regolamento prevede che il titolare dei dati lo faccia senza indebito ritardo e, in ogni caso, entro cinque giorni lavorativi, nel primo caso, cioè per rispondere a richieste di accesso legate ad un'emergenza pubblica, ed entro 30 giorni lavorativi in altri casi di necessità eccezionale.

I motivi per rigettare o per modificare una richiesta non sono a discrezione del soggetto privato, ma sono esplicitamente previsti dal comma 2 dell'art. 18. In via generale, i titolari dei dati possono farlo se la richiesta non soddisfa le condizioni previste dal regolamento, oppure – anche qualora la richiesta soddisfi tutte le condizioni – essi non

60. Si v. l'art. 14 del Regolamento (UE) 2023/2854.
61. Si v. l'art. 15 del Regolamento (UE) 2023/2854.
62. Si v. l'art. 17 del Regolamento (UE) 2023/2854.
63. Si v. l'art. 18 del Regolamento (UE) 2023/2854.

hanno il controllo sui dati richiesti o ancora nel caso in cui un altro ente pubblico abbia presentato in precedenza una richiesta analoga per la stessa finalità e al titolare dei dati non è stata notificata la cancellazione dei dati. In quest'ultimo caso il legislatore presume che gli enti pubblici possano poi agevolmente scambiarsi i dati tra loro.

Inoltre, a meno che l'archiviazione dei dati sia richiesta dall'ordinamento europeo o nazionale per garantire l'accesso ai documenti o per adempiere a specifici obblighi di trasparenza, le amministrazioni e gli enti pubblici hanno l'obbligo di cancellare i dati – informando il titolare e i soggetti che li hanno ricevuti – appena non siano più necessari per perseguire la finalità indicata[64].

Infine, per quanto riguarda il regime tariffario, in via generale, qualora la richiesta venga accolta e risponda ad un'emergenza pubblica, i titolari dei dati di medie e grandi dimensioni (non le micro e le piccole imprese) devono mettere a disposizione i dati necessari a titolo gratuito.

In questo caso, l'ente pubblico che ha ricevuto i dati, se richiesto dal titolare dei dati, gli fornisce in ritorno un riconoscimento pubblico. Invece, se la richiesta è legata ad una necessità sopravvenuta, il titolare dei dati ha diritto a un compenso equo per la messa a disposizione dei dati. Tale compenso copre i costi tecnici e organizzativi sostenuti per soddisfare la richiesta, compresi, se del caso, i costi di anonimizzazione, pseudonimizzazione, aggregazione e di adattamento tecnico, e un margine ragionevole. Su richiesta dell'ente pubblico, il titolare dei dati fornisce informazioni sulla base per il calcolo dei costi e del margine ragionevole[65].

Il regime di "apertura" e di riutilizzo dei dati in possesso dei soggetti privati previsto dal Regolamento (UE) 2023/2854, dunque, a differenza del regime generale previsto nella direttiva (UE) 2019/1024, certamente è lontano dall'idea originaria degli open data, ma, almeno in nuce, allarga il perimetro del paradigma dei dati aperti e contribuisce a superare l'idea che i dati di interesse pubblico da condividere siano solo quelli in possesso dei soggetti pubblici.

Basti pensare al semplice fatto che il regolamento abbia previsto, per la prima volta, una forma di funzionalizzazione dei dati di interesse pubblico in possesso dei privati per il raggiungimento di finalità generali, tanto da prevedere, in presenza di una richiesta, che i privati non siano completamente liberi di negare l'accesso ai dati e il loro riutilizzo, ma lo possano fare solo nei casi esplicitamente previsti dal regolamento. Inoltre, come alcune riflessioni hanno fatto emergere, è possibile considerare questo insieme di obblighi e oneri come un vero obbligo di servizio di interesse generale in capo ai soggetti privati, a garanzia di un diritto soggettivo e un interesse generale alla conoscenza, strumentale alla costruzione dell'identità personale e collettiva[66].

Si tratta, però, di un regime ancora molto condizionato, che permette l'accesso e il riutilizzo dei dati in possesso dei privati soltanto per specifiche finalità (emergenziali o di stretta necessità, che sono giustificate solo dopo l'impossibilità di percorrere soluzioni di mercato), non sempre gratuitamente (considerando che nei casi di maggiore frequenza si dovrà sottostare ad una tariffa) e, in particolare, con limiti di conservazione dei dati consistenti. Un regime che – seppur riconoscendo che i soggetti privati posseggono dati spesso necessari alla cura dei diritti e degli interessi collettivi – dimostra ancora scarsa attenzione ai bisogni conoscitivi delle amministrazioni pubbliche, in un contesto di forte asimmetria informativa che oggi esiste tra settore pubblico e settore privato[67].

64. Si v. l'art. 19 del Regolamento (UE) 2023/2854.

65. Si v. l'art. 20 del Regolamento (UE) 2023/2854.

66. In questo senso si v. Castaldo 2024, che sostiene come questi obblighi di servizio di interesse generale siano e che, considerando il nostro ordinamento, potrebbe avere anche un fondamento costituzionale nella promozione della cultura e del patrimonio culturale (art. 9, Cost.), nel diritto all'informazione e all'identità personale (artt. 21 e 22, Cost.), nella libertà di scienza (art. 33, Cost.), e più in generale nel principio personalista e di solidarietà (art. 2, Cost.).

67. Un'asimmetria evidenziata da tempo dalla letteratura scientifica. Si v. Cremona 2023, Falcone 2023, Betzu 2022, Betzu 2021, Pardolesi 2021.

3.4. Le finalità prevalentemente economiche dell'accesso e del riutilizzo dei dati di interesse pubblico

In ultimo, è utile soffermarci sulle finalità a cui l'apertura dei dati è preposta secondo le norme europee in analisi.

La disciplina europea ha rafforzato, in particolare con gli ultimi regolamenti, la sua finalità di fondo originaria, che aveva ispirato le prime direttive europee: quella della valorizzazione economica e commerciale dei dati di interesse pubblico, ma – a differenza delle prime direttive – in un contesto di complessiva liberalizzazione della circolazione dei dati nell'Unione europea.

Una tendenza evidente a partire dalle finalità che sono esposte sia nella direttiva (UE) 2019/1024 – che mira a garantire il riutilizzo il più possibile libero dell'informazione del settore pubblico o finanziata dal settore pubblico "al fine di promuovere l'utilizzo di dati aperti e di incentivare l'innovazione nei prodotti e nei servizi […]"[68] – sia del Regolamento (UE) 2023/2854 – che mira ad allargare ancora la platea delle categorie di dati interessati, fino ad allora esclusi, "al fine di agevolare l'utilizzo dei dati per la ricerca e l'innovazione europee da parte di soggetti pubblici e privati"[69].

In questa direzione va anche la motivazione di fondo che ha mosso il legislatore europeo nell'introduzione del divieto di prevedere obblighi di localizzazione dei dati non personali da parte degli Stati membri. Il Regolamento (UE) 2018/1807 vuole semplicemente liberalizzare la circolazione dei dati non personali, abolendo gli obblighi di localizzazione, in quanto "il presente regolamento non limita in alcun modo la libertà delle imprese di stipulare contratti che stabiliscano dove devono essere localizzati i dati. Il presente regolamento è inteso unicamente a salvaguardare tale libertà garantendo che il luogo stabilito possa trovarsi ovunque nell'Unione"[70].

Un approccio che, senza dubbio, è stato parzialmente mitigato da altre disposizioni, le quali fanno emergere dal disegno normativo complessivo anche finalità differenti da quelle strettamente economiche.

In primo luogo è l'art. 14, paragrafo 2 della stessa direttiva (UE) 2019/1024 che individua tra le motivazioni che giustificano l'individuazione di alcune categorie di dati come "serie di dati di elevato valore", quello di "valutare le loro potenzialità: a) nell'apportare importanti benefici socioeconomici o ambientali e servizi innovativi; b) nel beneficiare un numero elevato di utilizzatori, in particolare PMI; c) nel contribuire a generare proventi; e d) nell'essere combinata con altre serie di dati".

Inoltre, si pensi al c.d. altruismo dei dati, previsto dall'art. 2 del Regolamento (UE) 2022/868. Si sta parlando della possibilità di condividere volontariamente dati personali (da parte degli interessati) o dei dati non personali (da parte dei titolari dei dati, cioè i soggetti privati) "senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati" e soprattutto "per obiettivi di interesse generale". Lo stesso art. 2 fa menzione egli ambiti possibilmente coinvolti: ad esempio vengono citate "quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale"[71].

Una previsione che introduce un importante istituto di condivisione dei dati, che sicuramente arricchisce le finalità a cui il regolamento sulla governance dei dati è stato preposto, però, si pone "lateralmente" e al massimo in modo complementare alla disciplina dei dati aperti.

Infine, si pensi alle finalità pubbliche, prevalentemente in una situazione di emergenza o di particolare necessità degli enti pubblici, sottese all'ostensione dei dati di interesse pubblico da parte dei soggetti privati, contenute nel Regolamento (UE) 2023/2854.

68. Si v. l'art. 1 comma 1 della direttiva (UE) 2019/1024. Mette bene in evidenza come questa sia la finalità principale della direttiva del 2019 Gobbato 2020.
69. Si v. il Considerando 6 della Regolamento (UE) 2023/2854.
70. In questo senso va il Considerando 4 del Regolamento (UE) 2018/1807.
71. Si v. l'art. 2 del Regolamento (UE) 2022/868.

Dunque, è evidente come le regole sui dati aperti, in particolare dopo il Regolamento (UE) 2022/868 sulla governance dei dati, si pongano come obiettivo principale la creazione di un spazio europeo dei dati, inteso come uno spazio in cui circolano liberamente i dati per fini commerciali e non commerciali, ma dove la prima delle due finalità ha una chiara preminenza: non solo considerando la grande attenzione che i testi normativi le riserva, come abbiamo avuto modo di specificare, ma soprattutto tenendo in debito conto che l'idea di fondo è che i dati di interesse pubblico debbano costituire la "benzina" del "motore computazionale" delle imprese digitali[72].

4. I dati aperti come prezioso asset del mercato digitale e il ruolo di mera intermediazione delle amministrazioni pubbliche

In conclusione, il regime europeo di accesso e riutilizzo dei dati in possesso delle amministrazioni, o meglio, dei dati di interesse pubblico – se consideriamo anche le forme di apertura previste per i soggetti privati – è prevalente uno strumento di regolazione del mercato unico digitale, che si pone come obiettivo principale la crescita della concorrenza, attraverso una maggiore circolazione di dati ritenuti essenziali per lo sviluppo di nuovi servizi e prodotti.

Se la domanda di partenza di questo lavoro era chiedersi quante delle finalità originaria degli open data (valorizzazione economica, da un lato e accrescimento della democraticità tramite controllo democratico e partecipazione informata, dall'altro) siano contenute nelle norme europee, possiamo affermare che è prevalente e meglio presidiata solo la prima delle tre, cioè la valorizzazione commerciale ed economica dei dati di interesse pubblico.

Nonostante sia presente questa tensione tra attenzione allo sviluppo della libertà di iniziativa economica e il sostegno a finalità diverse, in particolare nelle disposizioni serventi logiche di circolazione solidaristiche dei dati[73], i profili di democrazia sostanziale – che rappresentano il nucleo giustificativo più importante della concezione dei dati come *commons* – non sono mai esplicitate chiaramente nelle norme europee: non è mai presente un richiamo esplicito alla partecipazione democratica alle decisioni pubbliche o al controllo democratico che i dati di interesse pubblico aperti permetterebbero di sviluppare e tenere vivi.

Più nel dettaglio, l'utilità dei dati aperti per il controllo democratico dell'operato delle amministrazioni pubbliche è presente solo in filigrana: come abbiamo dimostrato, questo può essere un effetto potenziale e indiretto della libera circolazione dei dati. Una finalità che – considerando che la disciplina europea è una disciplina "minima" – è rimessa prevalentemente alle discipline nazionali e che, in ogni caso, risulta essere molto complessa da perseguire. Anche negli ordinamenti dove essa è più marcata, come in quello italiano[74], il suo raggiungimento dipende dalla presenza di una forte mediazione informativa dei soggetti intermedi (di partiti, sindacati, associazioni e organizzazioni di cittadini), gli unici che in potenza possono avere

72. Sull'obiettivo generale di formare spazi di dati europei si v. Franca 2023. Emblematico in questo senso il Considerando 3 del Regolamento (UE) 2022/868: "Il presente regolamento dovrebbe mirare a sviluppare ulteriormente il mercato interno digitale senza frontiere e una società e un'economia dei dati antropocentriche, affidabili e sicure. La normativa settoriale a livello dell'Unione può sviluppare, adeguare e proporre elementi nuovi e complementari, a seconda delle specificità del settore, come nel caso della prevista normativa dell'Unione in materia di spazio europeo dei dati sanitari e di accesso ai dati dei veicoli. Taluni settori economici sono inoltre già disciplinati dalla normativa settoriale a livello dell'Unione che comprende norme in materia di condivisione di dati o di accesso ai dati a livello transfrontaliero o dell'Unione, ad esempio la direttiva 2011/24/UE del Parlamento europeo e del Consiglio nel contesto dello spazio europeo dei dati sanitari e i pertinenti atti legislativi in materia di trasporti, come i regolamenti (UE) 2019/1239 e (UE) 2020/1056, e la direttiva 2010/40/UE e la del Parlamento europeo e del Consiglio nel contesto dello spazio europeo dei dati sulla mobilità".

73. Tra chi sottolinea questa tensione profonda si v. Castaldo 2024 e Maglione 2022.

74. Si pensi al caso italiano. Nel nostro ordinamento, infatti, la disciplina dei dati aperti si è sostanzialmente sovrapposta a quella degli obblighi di pubblicazione, risultando, almeno sulla carta, direttamente strumentale al controllo democratico sull'operato delle amministrazioni. Per un approfondimento si v. i contributi contenuti in Ponti 2016 e Carloni 2014.

i mezzi e le risorse capaci di valorizzare a pieno i dati aperti. Un elemento che, in generale, non è mai accompagnato da norme che lo favoriscano o provino a presidiarlo meglio.

Allo stesso modo, il ritorno conoscitivo collettivo prodotto dall'utilizzo dei dati aperti a fini partecipativi è lasciato – forse inevitabilmente, considerando la base giuridica utilizzata dalle istituzioni europee – alla dinamica della ricerca scientifica e alla curiosità dei cittadini: non c'è nessun dispositivo normativo che favorisca un ritorno conoscitivo verso l'amministrazione. L'unico ritorno conoscitivo presente nella logica di mercato è quello che avviene tramite i servizi conoscitivi che i soggetti privati potrebbero offrire all'amministrazione, attraverso l'attività negoziale[75]. Un ritorno conoscitivo, quindi, fuori dalla logica degli open data e dai loro profili democratici.

L'assenza delle finalità non economiche del paradigma dei dati aperti, dunque, allontana la disciplina positiva europea sulla circolazione dei dati di interesse pubblico dal modello filosofico originario: oggi non possiamo dire che esiste pienamente un regime dei dati aperti, nonostante sia possibile ricavare dall'ordinamento un approccio diverso, anche di natura prescrittiva.

I dati aperti sono, di fatto, beni "essenziali" per l'esercizio di diritti (come il diritto di partecipazione alla decisione amministrativa e il diritto alla sua conoscibilità) corollari del principio di imparzialità (articolo 97 della Costituzione) e del diritto ad una buona amministrazione (riconosciuto come fondamentale dalla Carta di Nizza) e, allo stesso tempo, strumentali al corretto funzionamento del sistema democratico[76]. È auspicabile, dunque, un approccio diverso, che è possibile percorrere semplicemente prevendendo – al fine di raggiungere queste altre finalità – disposizioni che condizionano il regime sulla circolazione dei dati di interesse pubblico, così come sono state pensate per le serie di dati di elevato valore o nel *data governance act* per i dati pubblici soggetti a riservatezza privata.

Da ultimo, è necessario spendere due parole sul ruolo delle amministrazioni in questo contesto normativo.

Dalle norme europee emerge un modello di amministrazione intermediaria di dati e di informazioni pubbliche, proiettata principalmente a diffonderle e a farle circolare (non senza difficoltà e resistenze), più che ad utilizzarli pienamente nell'esercizio della funzione, in particolare come strumento di conoscenza della realtà e di identificazione e di soddisfazione dei propri bisogni conoscitivi[77].

Il risultato di queste scelte normative è che le amministrazioni sono portate ad organizzarsi per condividere i dati con le altre amministrazioni (italiane ed europee); per pubblicare le informazioni sui siti istituzionali e ad aprire le loro banche dati ai cittadini, in particolare ai poteri privati, che poi sono i veri utilizzatori degli open data; infine, per conformare il trattamento dei dati personali alle regole europee sulla protezione dei dati personali, in alcuni casi limitando la loro elaborazione a fini conoscitivi. Un'amministrazione intermediaria, dunque, che si limita a fornire i dati ai privati, anche sotto forma di servizio di interesse generale, ma senza valorizzare nessuno dei profili di democrazia sostanziale che appartengono intimamente alla logica originaria dei dati aperti[78]. Tra l'altro, un'amministrazione intermediaria sempre più in difficoltà, provata da anni di mancati investimenti e di drastica diminuzione di personale qualificato e di risorse strumentali, in particolari tecnologiche, per adempiere a questo compito[79].

Concludendo, se si volesse davvero attuare il paradigma dei dati aperti originario, è necessario non solo rivedere le norme, ma anche ripensare

75. Sull'esternalizzazione dei servizi informatici e informativi e sulla logica neoliberale sottesa a questo tipo di strumenti, che introducono surrettiziamente logiche private nell'esercizio delle funzioni pubbliche si v. Ponti 2024.

76. Su questo si v. Carloni 2022, Galetta 2019, Costantino 2015, Carloni 2014.

77. Un elemento che progressivamente sta emergendo attorno alla disciplina europea e nazionale sui sistemi di intelligenza artificiale e sull'emersione del nuovo paradigma di digitalizzazione ecosistemi amministrativi digitali. Per tutti si v. Carloni 2025 e Falcone 2023.

78. Nella letteratura sta emergendo in modo consistente l'idea che questo tipo di ostensione dei dati pubblici ai privati sia da considerare come un vero e proprio servizio pubblico. Per questo si v. Maglione 2022.

79. Per un'analisi sullo stato delle amministrazioni oggi si v. Merloni 2025.

il ruolo dell'amministrazione pubblica come semplice intermediario dei dati. L'amministrazione dovrebbe essere un soggetto informativo proattivo, in grado di interpretare diversamente il ruolo di soggetto che garantisce l'accesso e il riutilizzo dei dati in suo possesso, non limitandosi solo a rilasciare i dati, ma capace di incorporare nella sua azione di ostensione e di elaborazione dei dati tutte le finalità legati ai dati aperti, soprattutto i profili democratici del paradigma degli open data.

Riferimenti bibliografici

I. Alberti (2022), *La creazione di un sistema informativo unitario pubblico con la Piattaforma digitale nazionale dati*, in "Istituzioni del Federalismo", 2022

G. Arena (2022), *Da beni pubblici a beni comuni*, in "Rivista trimestrale di diritto pubblico", 2022, n. 3

C. Basunti (2024), *Nuove prospettive di valorizzazione dei dati in dimensione collettiva: le cooperative di dati (e le reti di impresa)*, in "Contratto e impresa", 2024, n. 3

M. Betzu (2022), *I baroni del digitale*, Editoriale Scientifica, 2022

M. Betzu (2021), *I poteri privati nella società digitale: oligopoli e antitrust*, in "Diritto Pubblico", 2021, n. 3

A. Bonomo (2012), *Informazione e pubbliche amministrazioni. Dall'accesso ai documenti alla disponibilità delle informazioni*, Cacucci, 2012

M. Bombardelli (2016), *La cura dei beni comuni come via di uscita dalla crisi*, in M. Bombardelli (a cura di), "Prendersi cura dei beni comuni per uscire dalla crisi. Nuove risorse e nuovi modelli di amministrazione", Editoriale Scientifica, 2016

C. Burelli (2025), *La scelta dell'atto da parte del legislatore dell'UE: il mercato unico digitale alla prova della qualità della legislazione*, in "federalismi.it", 2025, n. 28

E. Carloni (2025), *Critica dell'amministrazione artificiale*, il Mulino, 2025

E. Carloni (2022), *Il paradigma trasparenza. Amministrazioni, informazione, democrazia*, il Mulino, 2022

E. Carloni (2014), L*'amministrazione aperta. Regole strumenti limiti dell'open government*, Maggioli, 2014

G. Carullo (2025), *Dati, banche dati e interoperabilità dei sistemi informatici nel settore pubblico*, in R. Cavallo Perin, D.-U. Galetta (a cura di), "Il Diritto dell'Amministrazione Pubblica digitale", Giappichelli, II ed., 2025

G. Carullo (2019), *"Open Data" e partecipazione democratica*, in "Istituzioni del Federalismo", 2019, n. 3

R. Caso (2022), *Open Data, ricerca scientifica e privatizzazione della conoscenza*, in "Il Diritto dell'informazione e dell'informatica", 2022, n. 4-5

F. Casolari, C. Buttaboni, L. Floridi (2023), *The EU Data Act in context: a legal assessment*, in "International Journal of Law and Information Technology", vol. 31, 2023, n. 4

C. Castaldo (2024), *Libertà individuali e open data. Gli obblighi di servizio pubblico nella gestione dei dati*, Giappichelli, 2024

R. Cavallo Perin (2021), *Il contributo italiano alla libertà di scienza nel sistema delle libertà costituzionali*, in "Diritto amministrativo", 2021, n. 3

V. Cerulli Irelli (2022), *Proprietà, beni pubblici, beni comuni*, in "Rivista trimestrale di diritto pubblico", 2022, n. 3

A. Ciervo (2013), *I beni comuni*, Ediesse, 2013

F. Cortese (2021), *Come disciplinare l'amministrazione digitale?*, in A. Bartolini, T. Bonetti, B. Marchettiet al. (a cura di), "La legge n. 241 del 1990, trent'anni dopo", Giappichelli, 2021

F. Cortese (2016), *Che cosa sono i beni comuni?*, in M. Bombardelli (a cura di), "Prendersi cura dei beni comuni per uscire dalla crisi. Nuove risorse e nuovi modelli di amministrazione", Editoriale Scientifica, 2016

F. Costantino (2015), *Open Government, in Digesto delle discipline pubblicistiche*. Aggiornamento, Utet, 2015

E. Cremona (2023), *I poteri privati nell'era digitale. Libertà costituzionali, regolazione del mercato, tutela dei diritti*, Editoriale Scientifica, 2023

I. D'Elia (2006), *La diffusione e il riutilizzo dei dati pubblici. Quadro normativo comunitario e nazionale: problemi e prospettive*, in "Informatica e diritto", 2006, n. 1

F. Di Mascio (2017), *Miti e realtà degli "open data" all'italiana*, in "Giornale di diritto amministrativo", 2017, n. 3

M. Di Masi (2022), *Ripensare il cibo come bene comune*, in "Rivista critica del diritto privato", 2022, n. 1

D. Donati (2024), *Dai beni comuni al benessere comunitario. Evidenze, incertezze e limiti di un concetto sotto osservazione*, in D. Donati (a cura di), "La cura dei beni comuni tra teoria e prassi. Un'analisi interdisciplinare", FrancoAngeli, 2024

M. Falcone (2023), *Ripensare il potere conoscitivo pubblico tra algoritmi e big data*, Editoriale Scientifica, 2023

M. Falcone (2017), *Le potenzialità conoscitive dei dati amministrativi nell'era della "rivoluzione dei dati": il caso delle politiche di eradicazione dell'epatite C*, in "Istituzioni del Federalismo", 2017, n. 2

M. Falcone (2016), *Dati aperti e diritto al riutilizzo delle informazioni: la declinazione italiana del paradigma degli open data*, in B. Ponti (a cura di), "Nuova trasparenza amministrativa e libertà di accesso alle informazioni", Maggioli, 2016

S. Franca (2023), *I dati personali nell'Amministrazione pubblica. Attività di trattamento e tutela dei privati*, Editoriale Scientifica, 2023

D.-U. Galetta (2019), *"Open Government", "Open Data" e azione amministrativa*, in "Istituzioni del Federalismo", 2019, n. 3

S. Gatti (2024), *Dalla portabilità alle "portabilità": l'evoluzione al plurale di un diritto (e concetto) chiave nella disciplina europea dei dati*, in "European Journal of Privacy Law & Technologies", 2024, n. 1

S. Gobbato (2020), *Verso l'attuazione della direttiva (UE) 2019/1024 sul riutilizzo degli open data della PA: nuove opportunità per le imprese*, in "MediaLaws", 2020, n. 2

F. Goggiamani (2005), *La doverosità della pubblica amministrazione*, Giappichelli, 2005

M. Kurz (2023), *The Market Power of Technology. Understanding the Second Gilded Age*, Columbia University Press, 2023

A. Licastro (2025), *La configurazione dei mercati digitali a partire dal "Digital Markets Act"*, in "Rivista della regolazione dei mercati", 2025, n. 1

C. Lobascio (2023), *Tabella riassuntiva dell'evoluzione del diritto europeo dei dati e delle piattaforme*, in "Rivista italiana di informatica e diritto", 2023, n. 2

P.S. Maglione (2022), *L'"apertura" dei dati come servizio pubblico: spunti ricostruttivi alla luce della nuova disciplina sul riutilizzo dell'informazione del settore pubblico*, in "Il diritto dell'economia", 2022, n. 2

M.R. Marella (2017), *The* Commons *as a Legal Concept*, in "Law Critique", 2017, n. 28

M.R. Marella (a cura di) (2012), *Oltre il pubblico e il privato. Per un diritto dei beni comuni*, Ombre Corte, 2012

D. Marongiu (2008), *I dati delle pubbliche amministrazioni come patrimonio economico nella società dell'informazione*, in "Informatica e diritto", 2008, n. 1-2

D. Marongiu (2005), *La funzione di coordinamento informatico: Autonomia delle Regioni e poteri del Ministro per l'innovazione e le tecnologie, nota a C. Cost. 10-16 gennaio 2004, n. 17*, in "Il diritto dell'informazione e dell'informatica", 2005

U. Mattei (2020), *Prime note critiche sull'informazione come bene comune*, in "Rivista critica del diritto privato", 2020, n. 1-2

U. Mattei (2011), *Beni comuni. Un manifesto*, Laterza, 2011

G. Mazzei (2023), *"Big data" come beni comuni globali e principi in tema di "public utilities"*, in "federalismi.it", 2023, n. 12

F. Merloni (2025), *Diritti e pubbliche amministrazioni nell'austerità liberista. Storia di un abbandono*, Editoriale Scientifica, 2025

F. Merloni (2008), *Coordinamento e governo dei dati nel pluralismo amministrativo*, in B. Ponti (a cura di), "Il regime dei dati pubblici. Esperienze europee e ordinamento nazionale", Maggioli, 2008

A. Morace Pinelli (2024), *Dalla "Data Protection" alla "Data Governance": il Regolamento UE 2022/868*, in "La Nuova Giurisprudenza Civile Commentata", 2024, n. 2

E. Ostrom, C. Hess (a cura di) (2009), *La conoscenza come bene comune. Dalla teoria alla pratica*, Mondadori, 2009

R. Pardolesi (2021), *Piattaforme digitali, poteri privati e concorrenza*, in "Diritto pubblico", 2021, n. 3

M. Pathak (2024), *Data Governance Redefined: The Evolution of EU Data Regulations from the GDPR to the DMA, DSA, DGA, Data Act and AI Act*, in "European Data Protection Law Review (EDPL)", vol. 10, 2024, n. 1

O. Pollicino (2023), *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in "Quaderni costituzionali", 2023, n. 3

B. Ponti (2024), *Il fornitore dell'algoritmo quale soggetto estraneo all'amministrazione*, in "Rivista italiana di informatica e diritto", 2024, n. 2

B. Ponti (2023), *Attività amministrativa e trattamento dei dati personali. Gli standard di legalità tra tutela e funzionalità*, FrancoAngeli, 2023

B. Ponti (2019), *La mediazione informativa nel regime giuridico della trasparenza: spunti ricostruttivi*, in "Diritto dell'informazione e dell'informatica", 2019, n. 2

B. Ponti (a cura di) (2016), *Nuova trasparenza amministrativa e libertà di accesso alle informazioni*, Maggioli, 2016

B. Ponti (2013), *Il regime dei dati oggetto di pubblicazione obbligatoria: i tempi, le modalità, ed i limiti della diffusione; l'accesso civico; il diritto al riutilizzo (art. 4, 5, 7-9, 52 comma 2 e 3, 53)*, in B. Ponti (a cura di), "La trasparenza amministrativa dopo il d. lgs. 14 marzo 2013, n. 33", Maggioli, 2013

B. Ponti (2011), *Open Data and Transparency: A Paradigm Shift*, in "Informatica e diritto", 2011, n. 1-2

B. Ponti (2008), *Titolarità e riutilizzo dei dati pubblici*, in B. Ponti (a cura di), "Il regime dei dati pubblici. Esperienze europee e ordinamento nazionale", Maggioli, 2008

B. Ponti (2007), *Il patrimonio informativo pubblico come risorsa. I limiti del regime italiano di riutilizzo dei dati delle pubbliche amministrazioni*, in "Diritto Pubblico", 2007, n. 3

N. Purtova, G. van Maanen (2023), *Data as an economic good, data as a commons, and data governance*, in "Law Innovation Technologies", vol. 16, 2023, n. 1

M. Renna, C. Miccichè (2022), *Beni pubblici e diritti d'uso pubblico. La resilienza delle prerogative collettive al mutare dei modelli di sviluppo*, in "Rivista trimestrale di diritto pubblico", 2022, n. 3

G. Resta (2022), *Pubblico, privato e collettivo nel sistema europeo di governo dei dati*, in "Rivista trimestrale di diritto pubblico", 2022, n. 4

G. Resta (2013), *La conoscenza come bene comune: quale tutela?*, in Aa.Vv., "Tempo di beni comuni. Studi multidisciplinari", Ediesse, 2013

G. Resta (2011), *La privatizzazione della conoscenza e la promessa dei beni comuni: riflessioni sul caso "Myriad Genetics,* in "Rivista critica del diritto privato", 2011

A. Ricci (2024), *Introduzione al regolamento europeo sull'accesso equo ai dati e sul loro utilizzo*, in "Le Nuove leggi civili commentate", 2024, n. 4

S. Rodotà (2013), *Il terribile diritto. Studi sulla proprietà privata e i beni comuni*, il Mulino, 2013

S. Rossa (2021), *Contributo allo studio delle funzioni amministrative digitali. Il processo di digitalizzazione della Pubblica Amministrazione e il ruolo dei dati aperti*, Wolters Kluwer-CEDAM, 2021

L. Ruggeri (2023), *La dicotomia dati personali e dati non personali: il problema della tutela della persona nei c.dd. dati misti*, in "Il Diritto di famiglia e delle persone", 2023, n. 2

A. Simonati (2025), *I dati personali in possesso dell'amministrazione: beni a destinazione pubblica?*, in "CERIDAP", 2025, n. 3

A. Simonati (2018), *La ricerca in materia di trasparenza amministrativa: stato dell'arte e prospettive future*, in "Diritto amministrativo", 2018, n. 2

C. Simone, A. Laudando (2025), *Principles and obligations of the Digital Markets Act in regulating the economic power of gatekeepers: Positive, negative or trade-off effects?*, in "Electron Markets", vol. 35, 2025

D. Solda-Kutzman (2011), *Public Sector Information Commons*, in "Informatica e diritto", 2011, n. 1-2

S. Torregiani (2020), *Il dato non personale alla luce del Regolamento (UE) 2018/1807: tra anonimizzazione, "ownership" e "Data by Design"*, in "federalismi.it", 2020, n. 18

G. van Maanen, C. Ducuing, T. Fia (2024), Data *commons*, in "Internet Policy Review", vol. 13, 2024, n. 2

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0258 • articolo non sottoposto a peer review • pubblicato in anteprima il 21 gen. 2026

Anna Simonati

Considerazioni di sintesi. Funzione amministrativa ed esigenze del mercato. La gestione dei dati in ambito pubblico tra complessità e complicazione

L'Autrice è professoressa ordinaria in Diritto amministrativo all'Università di Trento

Questo contributo fa parte della sezione monografica *I dati in ambito pubblico tra esercizio della funzione amministrativa e regolazione del mercato*, a cura di Marco Bombardelli, Simone Franca, Anna Simonati

La cifra che nel nostro ordinamento attualmente caratterizza il trattamento dei dati, soprattutto se personali, è la complessità. La disciplina di portata generale è stata via via arricchita di nuovi tasselli ed è stata progressivamente affiancata da disposizioni settoriali di varia natura (per esempio nel campo dei contratti pubblici, della cybersicurezza e dei dati sanitari). La sottoposizione – almeno parziale – dei soggetti pubblici alla normativa sul trattamento dei dati personali risponde a un'esigenza forte e costituzionalmente radicata nell'ordinamento, che mira in primo luogo a evitare di incorrere nella violazione della riservatezza delle persone coinvolte. Al contempo, tuttavia, tale doverosa precauzione espone il sistema (come è emerso con cristallina chiarezza dal contributo di Fabio Francario) a un potenziale paradosso. È fondamentale, infatti, evitare che la necessità di vigilare affinché non si consumino indebite violazioni "ingessi" in maniera eccessivamente invasiva lo svolgimento dei compiti istituzionali e, di conseguenza, il perseguimento dell'interesse pubblico, che resta l'obiettivo primario di qualsiasi attività amministrativa.

Il soddisfacimento di tale esigenza di flessibilità non è sicuramente agevolato dalla compresenza di due livelli normativi, quello sovranazionale e quello nazionale, la cui convivenza è a tratti difficile. Anzi, su questo fronte, deve registrarsi una sorta di recesso del secondo a vantaggio del primo, come ha ben evidenziato Francesco Midiri. Ciò non concerne soltanto profili strettamente organizzativi o comunque di natura marcatamente applicativa, ma anche il rapporto fra diritti (potenzialmente, di rilievo costituzionale) e, dunque, fra valori. Infatti, la prospettiva sistematica assunta dall'ordinamento nazionale (tendenzialmente incentrato sulla protezione delle posizioni individuali) e da quello eurounitario (che invece innegabilmente si concentra maggiormente sulla salvaguardia della concorrenza, dunque su una prospettiva più generale e, per così dire, "collettiva") evidentemente non coincidono perfettamente. La disponibilità del legislatore statale a compiere un passo indietro potrebbe dunque produrre effetti allarmanti proprio sul piano della tutela dei diritti inviolabili delle persone, ove è indispensabile la predisposizione di adeguati presidi.

In alcuni campi, invero, la difficoltà del rapporto fra livello normativo europeo e livello normativo nazionale è particolarmente evidente. Fra i settori "sensibili" spicca ad esempio quello della cybersecurity. In quest'area, emerge un ulteriore elemento di complicazione, che deriva dal fatto che la gestione dei dati (in particolare, di quelli personali) nell'ambito del cyberspazio comporta una dilatazione pressoché incontrollabile del numero degli utenti interessati, il che determina, di conseguenza, l'intreccio e a tratti la sovrapposizione di regole, provenienti da ordinamenti diversi. Diventa allora a maggior ragione cruciale il momento organizzativo, soprattutto in relazione alla costituzione di interlocutori istituzionali omogenei nei vari sistemi, idonei a interagire su basi (se non perfettamente uniformi) quanto meno tendenzialmente comparabili sul piano concettuale. È evidente che il contributo su questo fronte delle strutture sovranazionali già esistenti (in primo luogo, naturalmente, quelle di matrice europea) può essere preziosissimo. Sarebbe del resto errato – soprattutto laddove sono coinvolti diritti fondamentali dei singoli – dare per scontato che vi sia spazio esclusivamente per i parametri di salvaguardia accolti nel mondo occidentale; deve riconoscersi, però, che al momento a questo fa prevalentemente riferimento il mercato, che di per sé sembrerebbe incentivare la massima circolazione dei dati, indiscutibilmente concepiti anche come beni dotati di valore economico. Per quanto concerne specificamente l'ordinamento italiano, poi, il problema della corretta gestione dei dati personali nel cyberspazio si innesta sul processo di lenta ma progressiva trasformazione dell'azione amministrativa verso modalità telematiche, che richiede l'attivazione di idonee iniziative per l'alfabetizzazione tecnologica della popolazione.

Alla multiformità delle regole sul trattamento dei dati, si aggiunge un altro fattore di complicazione, che consiste, per così dire, nell'elasticità delle regole stesse. Infatti, nonostante si tratti di un *corpus* normativo piuttosto consistente e spesso composto da disposizioni assai dettagliate nel contenuto, in realtà quasi mai esse vanno a costituire nuclei precettivi realmente autosufficienti. Al contrario, all'interprete è quasi sempre lasciato un ambito, più o meno ampio a seconda dei casi, di creatività nel momento dell'implementazione, il che talora può incidere negativamente sul livello di efficienza complessiva del sistema.

Si può riscontrare, a ben vedere, anche in questo caso una sorta di paradosso: alla maggiore flessibilità normativa dovrebbe corrispondere la maggiore propensione dei meccanismi giuridici ad adattarsi alle esigenze concrete. Tuttavia, è innegabile che una legalità a maglie (eccessivamente) larghe possa risultare controproducente. Ciò pare verificarsi con particolare evidenza nell'ipotesi della disciplina della gestione dei dati da parte di soggetti privati economicamente e socialmente particolarmente forti, il cui operato dovrebbe comunque essere risolutamente indirizzato verso parametri costituzionalmente orientati nella prospettiva della tutela dei diritti.

Non va sottaciuto, però, che la contraddizione fra l'anelito alla semplificazione – che dichiaratamente costituisce attualmente il macro-obiettivo perseguito dal legislatore – e la moltiplicazione degli attori e dei livelli di regolazione assume una connotazione specifica con riferimento ai trattamenti svolti dai soggetti pubblici. Anche alla pubblica amministrazione, infatti, si applica in linea di principio – come ai soggetti privati – il parametro della stretta necessità rispetto al fine perseguito. A seguito dell'entrata in vigore del GDPR del 2016, tuttavia, questa regola si sovrappone non senza incertezze al parametro della legalità rispetto all'attribuzione dei compiti istituzionali, in cui i singoli trattamenti vanno inquadrati. Ciò significa – come ha sottolineato Benedetto Ponti – che, nel settore pubblicistico, sul piano operativo le regole di minimizzazione dei rischi e di stretta necessarietà del trattamento, intercettando i principi di legalità, competenza e tipicità dei poteri pubblici, non possono non declinarsi nel paradigma della proporzionalità e della ragionevolezza dell'attività amministrativa.

Inoltre, proprio il principio di competenza comporta una ripartizione fra vari soggetti delle attribuzioni pubbliche connesse al trattamento dei dati, il che richiede, sul piano organizzativo, l'attivazione di circuiti comunicativi efficienti fra centri di potere. In altri termini, l'impianto tradizionale dei rapporti fra autorità, essenzialmente basato sulla rigida delimitazione dei confini tra i ruoli di ciascuno, dovrebbe lasciare il posto a un impianto più dinamico, in cui una maggiore osmosi informativa si coniughi comunque con la rigorosa adesione da parte di tutti i soggetti pubblici coinvolti alle regole per la difesa dei diritti individuali. Per questo è probabilmente indispensabile dotare la stessa amministrazione, globalmente intesa, di strumenti per la migliore comprensione e gestione delle questioni applicative.

Nel rapporto con le regole del mercato si profilano le maggiori insidie connesse con il trattamento dei dati, che dipendono in massima parte dall'accoglimento di una concezione riduttiva, e in parte fuorviante, fondata essenzialmente sul supposto valore prevalentemente economico delle informazioni. Anche in questa prospettiva, l'analisi dell'ordinamento italiano non può prescindere del tutto dall'attenzione per le regole di matrice eurounitaria, suscettibili di vincolare il legislatore nazionale.

Come in parte già si è evidenziato, nel contesto europeo di fatto le regole pensate per i trattamenti da parte dei soggetti pubblici sono una sorta di gemmazione da quelle pensate per i trattamenti da parte di privati. Ma dalla frequente assunzione di una prospettiva prevalentemente "mercantilistica", in base alla quale il dato è visto in primo luogo come bene destinato allo scambio negoziale, deriva la scarsa valorizzazione del fattore – che invece dovrebbe essere cruciale – della funzionalizzazione all'interesse pubblico del trattamento. Inoltre, si profila un rischio che deriva direttamente dalla patrimonializzazione strisciante del dato: l'idea della disponibilità del diritto alla riservatezza dietro corrispettivo di un compenso economico. Di conseguenza (e non a caso), l'accento normativo negli anni recenti si è gradualmente ma inesorabilmente spostato proprio dalla tutela della riservatezza (diritto inviolabile individuale riconducibile all'art. 2 Cost.) alla disciplina del trattamento dei dati personali altrui, oggetto di un (parzialmente diverso) diritto all'autodeterminazione informativa. Quest'ultimo, infatti, più facilmente può essere ricondotto all'alveo della disponibilità patrimoniale in senso ampio.

Se questo è vero, si può riscontrare un ulteriore paradosso, che si affianca a quelli già individuati, nella equiparazione (solo apparente) fra proprietà e appartenenza, poiché nel settore dell'utilizzo dei dati da parte dell'amministrazione vi sono diversi livelli di controllo sull'oggetto del trattamento. Il primo (ma non l'unico) è quello che può essere esercitato dal titolare dei dati; costui, tuttavia, non può in realtà vantare alcuna esclusiva sull'utilizzo del proprio patrimonio informativo. Pertanto, se ne può in via tendenziale essere considerato il "proprietario", lo è solo parzialmente e con un ampio margine di approssimazione. Anzi, nei vari livelli di "stratificazione" giuridica che li contraddistinguono, gli istituti riconducibili alla complessa nozione di appartenenza coinvolgono anche altri soggetti: l'amministrazione in quando depositaria "di primo livello" (e custode della legalità del trattamento, mediante l'intervento mirato dei Garanti), ma anche le imprese e gli operatori del mercato che aspirano a utilizzare i dati a fini di lucro. In quest'ottica, riflettendo sulla relazione fra il singolo (titolare del dato personale), il potere pubblico e il mercato, è possibile riscontrare come, in realtà, il vero antagonista della tutela dei diritti individuali spesso non sia tanto il potere pubblico quanto piuttosto lo strapotere in via di fatto del mercato. Infatti, se rispetto al primo possono suscitare timore eventuali derive autoritarie, queste appaiono comunque fronteggiabili mediante lo strumentario rimediale – per quanto parziale e ancora imperfetto – predisposto dall'ordinamento. Lo strapotere in via di fatto del mercato risulta, invece, ben più pericoloso, perché suscettibile di imporsi a prescindere dall'adesione a moduli comportamentali precostituiti e improntati alla tutela degli interessi di tutte le parti coinvolte.

Le ripercussioni negative in termini di certezza del diritto, derivanti dalla moltiplicazione di livelli normativi non perfettamente omogenei e coerenti, sono particolarmente evidenti con riferimento alla rilevanza del consenso al trattamento del titolare dei dati. Per quanto concerne i rapporti interprivatistici, si osserva che, nonostante tale consenso sia di regola un presupposto indispensabile, esso subisce di fatto una sorta di "dequotazione" a causa dell'approccio prevalentemente "mercantilistico" che contraddistingue l'evoluzione della disciplina.

La necessità di ottenere il consenso del titolare dei dati non è invece prevista in relazione ai trattamenti svolti dai soggetti pubblici, che sostanzialmente trovano legittimazione autosufficiente nella previsione normativa e nel legame con il perseguimento di una funzione preordinata al soddisfacimento dell'interesse della collettività. A ben vedere, questa non è invero una peculiarità isolata: l'assenza della necessità del coinvolgimento del titolare delle informazioni in vista del loro utilizzo si ravvisa, infatti, anche in un'altra fattispecie, normata in epoca assai più risalente, precisamente nella legge n. 241/1990. Si tratta della possibilità, concessa alle autorità pubbliche *ex* art. 22, c. 5, di mettere a disposizione l'una dell'altra senza particolari formalità i documenti in loro possesso, se pur contenenti informazioni riservate di soggetti privati. È evidente che, anche in questo caso, la *ratio* della scelta operata dal legislatore è riposta nell'intrinseca funzionalizzazione al perseguimento dell'interesse della collettività che contraddistingue l'operato dei soggetti pubblici.

La disciplina dell'intermediazione dei dati, tuttavia, sembra essere basata in modo abbastanza acritico e indiscriminato sulla logica del consenso, il che – come giustamente ha rilevato Fabio Bravo – certamente introduce un elemento di complicazione aggiuntivo. Del resto, è ragionevole escludere che l'amministrazione possa, in base alle norme sull'intermediazione, trattenere – in forza esclusivamente del consenso del titolare – dati personali il cui trattamento non rientrerebbe fra i suoi compiti istituzionali. Pare doversi ritenere, infatti, che sia comunque valida la condizione generale di ammissibilità del trattamento esclusivamente laddove questo sia riconducibile alle funzioni dell'ente che lo svolge.

Ancora, fra i numerosi paradossi che caratterizzano il trattamento dei dati da parte dell'amministrazione, emerge, mi pare, quello relativo alla piena estrinsecazione del principio di trasparenza, che si arricchisce di sfaccettature semantiche complesse, in particolare, allorché lo si pone in relazione con la pubblicità dell'azione della pubblica amministrazione.

È ancora assai attuale, in proposito, la notissima sentenza della Corte costituzionale n. 20/2019 sull'obbligo di pubblicazione dei compensi percepiti dai dirigenti, in cui la Consulta ha paventato possibili effetti controproducenti – precisamente, sotto forma di "opacità per confusione" – delle disposizioni che impongono massicciamente la pubblicazione indiscriminata di considerevoli quantità di dati. Pertanto,

nel concetto di *accountability*, che deve guidare l'operato delle istituzioni, rientra anche l'assunzione di responsabilità (almeno entro certi limiti) circa la selezione degli elementi conoscitivi meritevoli di divulgazione, nell'ottica non solo del puntuale rispetto della normativa vigente, ma anche dell'effettività della trasparenza nella sua più ampia accezione di comprensibilità dell'azione amministrativa.

Il problema si pone con peculiare intensità nel caso del trattamento di *open data*, di cui si è occupato Matteo Falcone. Una prima questione aperta è di carattere sistematico. Ci si può chiedere, infatti, se il dovere della pubblica amministrazione di mettere a disposizione della collettività gli *open data* corrisponda allo svolgimento di una funzione o all'erogazione di un servizio. Anche a prescindere dalla soluzione ritenuta preferibile, non può sottovalutarsi la netta dicotomia fra i trattamenti svolti direttamente dalle istituzioni e quelli che poggiano, invece, sulla collocazione dei dati sul mercato, che potrebbe risultare difficilmente conciliabile con il perseguimento dell'interesse pubblico e con la piena protezione anche dei soggetti più vulnerabili. Diventa dunque cruciale l'attenzione per il riconoscimento di una funzione pubblica in parte nuova (almeno, in quanto tale) quale quella di comunicazione pubblica, preludio a qualsiasi meccanismo per l'esercizio efficiente (diretto o indiretto) del potere.

La trasparenza è fondamentale soprattutto in settori di per sé "sensibili", come quello del trattamento dei dati sanitari, su cui si è soffermato Stefano Corso. In tale ambito, la consapevolezza del titolare del dato è davvero cruciale ed è pertanto essenziale (come avviene in generale, ma a maggior ragione e con particolare intensità in questo campo) calibrare l'attività di gestione dei dati personali sui principi di ragionevolezza e proporzionalità. Peraltro, alla luce delle riforme legislative più recenti in materia, non può non rilevarsi come il tema del trattamento dei dati sanitari intercetti quasi immancabilmente quello del loro trattamento con modalità digitali.

Ma, anche al di fuori dell'ambito sanitario, l'informatizzazione delle modalità di svolgimento del trattamento (paradossalmente, originariamente pensata dal legislatore nazionale come fonte di semplificazione, almeno in parte) si scontra con una serie di problematiche applicative, connesse soprattutto alla scarsa alfabetizzazione telematica della popolazione italiana, che rende piuttosto arduo l'esercizio effettivo di quel diritto all'autodeterminazione informativa che dovrebbe rappresentare il nocciolo duro del diritto alla riservatezza individuale a fronte dei trattamenti svolti dalla pubblica amministrazione.

Analogamente, a maggior ragione, nel caso della gestione di enormi quantità di dati (*big data*), tipica dell'era del cosiddetto "capitalismo informazionale", nel momento in cui taluno – poniamo, anche volontariamente – fornisce a terzi un dato che lo riguarda, non sempre, pur a fronte di un'adeguata informativa, sarà in grado di capire con quali altri dati esso sarà messo in relazione; il risultato concreto potrebbe consistere nella formazione di un'informazione assai complessa, potenzialmente utilizzabile anche a fini discriminatori (per esempio, su basi economico-sociali o strettamente reddituali, a seguito di profilazione). I rischi sono particolarmente evidenti con riferimento ai trattamenti svolti dalle autorità amministrative, data la (già richiamata) tendenziale osmosi senza formalità rigorose fra banche dati pubblicistiche e data la (anch'essa già richiamata) dequotazione in quest'ambito del ruolo del consenso del titolare dei dati. La situazione si aggrava inevitabilmente allorché, a partire dalla progressiva informatizzazione delle attività istituzionali in ossequio al principio *digital first*, l'anelito alla semplificazione conduce all'elisione degli adempimenti procedimentali dialogici ed esplicativi, che in via esclusiva e insostituibile consentirebbero ai cittadini di acquisire la necessaria consapevolezza sull'utilizzo dei dati.

A ciò corrisponde, quasi inevitabilmente, un depauperamento strisciante dei meccanismi rimediali, di cui l'ordinamento italiano si è dotato in maniera certamente non esaustiva. Soprattutto, desta qualche preoccupazione la circostanza che l'intricata normativa vigente renda in concreto particolarmente arduo il pieno accesso al fatto da parte delle autorità chiamate a dirimere le controversie in materia di trattamento dei dati. Su questo fronte, anzi, pare di poter dire che il titolare dei dati sottoposti a trattamento da parte della pubblica amministrazione ha a propria disposizione un solo meccanismo difensivo realmente efficace, che è di natura essenzialmente risarcitoria. Si tratta invero, tuttavia, di un'arma "spuntata", destinata a operare sempre *a posteriori*, senza poter evitare la lesione.

Anche questo è un elemento non nuovo del sistema normativo: lo stesso meccanismo rimediale predisposto tradizionalmente in materia di accesso documentale *ex* art. 25, legge n. 241/1990, pur constando di

un arsenale potenzialmente eterogeneo che si compone di strumenti di natura sia giustiziale sia giurisprudenziale in senso stretto, risulta orientato essenzialmente a proteggere l'interesse dell'istante che aspira all'ostensione della documentazione. Se, invece, la violazione delle regole ha determinato un ingiustificato assenso alla richiesta di accesso, una volta che il dato sia stato indebitamente comunicato o addirittura pubblicato non c'è quasi mai margine di tutela, se non, appunto, sul fronte risarcitorio. Nonostante – come ha bene evidenziato Simone Franca – la giurisprudenza ordinaria abbia tentato di effettuare un oculato bilanciamento fra le esigenze contrapposte nelle fattispecie concrete, mancano istituti idonei a valorizzare la *mission* giuspubblicistica complessiva dell'operato dell'amministrazione. Quest'ultima si estrinseca, in prima battuta, nella doverosità – in base ai principi di legalità e competenza – dei trattamenti direttamente svolti dai soggetti pubblici. Non è meno rilevante, però, il ruolo di garanzia "preventiva" delle autorità, cui spetta contribuire alla protezione degli individui (soprattutto di quelli più vulnerabili e meno attrezzati all'autodifesa) a fronte dei trattamenti potenzialmente assai invasivi effettuati da terzi, in particolare se con finalità strettamente imprenditoriali. Si pone dunque il problema dell'alfabetizzazione anche della pubblica amministrazione nel momento in cui è chiamata a interagire con questi soggetti, dotati di un know how e di obiettivi ben diversi dal perseguimento dell'interesse pubblico.

Forse (anche) per questo negli anni recenti, nel contesto delle autorità amministrative, i cosiddetti Garanti hanno di fatto ampliato il loro ruolo, assumendo atteggiamenti interventisti, in particolare mediante l'emanazione di linee guida, suscettibili di incidere sulle modalità concrete del trattamento dei dati da parte dell'amministrazione.

Al di là delle difficoltà di collocazione sistematica di tali strumenti, va tenuto presente che ciascuna autorità garante è depositaria di un interesse pubblico specifico, la cui protezione rappresenta una *mission*, per così dire, "monolitica". Di conseguenza, l'approccio al problema da parte dei Garanti è in un certo senso "ciclopico": molto concentrato sulle specificità settoriali, ma spesso privo di attenzione adeguata alla lettura sistemica dei vari elementi rilevanti.

È peraltro interessante che negli atti dei Garanti si punti molto sulla necessità di assicurare misure di carattere organizzativo, in modo che, nell'ambito di ciascuna struttura amministrativa incaricata del trattamento di dati, vi siano competenze istituzionali specializzate. Pertanto, anche su questo fronte emerge il profilo della tensione fra complessità e semplificazione, per quanto in questo caso la maggiore "complicazione" organizzativa potrebbe effettivamente portare a risultati fruttuosi in termini di efficienza complessiva del sistema, consentendo una maggiore consapevolezza delle scelte operative.

Più in generale, permane indubbiamente il rischio che la complessità produca in realtà complicazione fine a sé stessa. Di questo pericolo sembra essere stato pienamente consapevole, del resto, il legislatore degli anni Novanta del Ventesimo secolo, il quale, nell'art. 18 della legge n. 675/1996 (primo sforzo normativo esaustivo e sistematico in materia di tutela della riservatezza) – in maniera lungimirante – aveva qualificato il trattamento di dati personali come attività pericolosa *ex* art. 2050 cod. civ., prevedendo di conseguenza l'inversione dell'onere probatorio nelle cause di natura risarcitoria intentate dal titolare delle informazioni danneggiato dal trattamento indebito. Questa scelta, con gli occhi dell'interprete odierno, può apparire addirittura profetica: sempre più pericolosa, infatti, appare obiettivamente questa attività dal punto di vista della pubblica amministrazione.

La complessità dell'attività amministrativa in materia di trattamento dei dati, peraltro, può produrre ulteriori ripercussioni non irrilevanti rispetto alla natura del potere esercitato. Mentre tempo fa (negli anni Novanta del secolo scorso e fino ai primi anni Duemila) c'era spazio per la qualificazione dell'azione amministrativa in materia di trasparenza essenzialmente in termini di rigorosa applicazione (previa interpretazione complessa) della normativa vigente – essendo i casi di discrezionalità assai circoscritti, specificamente alle fattispecie di differimento dell'esercizio del diritto di accesso ai documenti per esigenze pubblicistiche di efficienza – oggi la situazione appare, se non diametralmente opposta, certamente assai diversa e diversificata. Pare di poter dire, infatti, che la quantità e la qualità dei fattori sottesi alle determinazioni sulla gestione del patrimonio informativo nella disponibilità dell'amministrazione abbia di fatto trasformato profondamente la natura del suo intervento deliberativo, tanto che quasi sempre attualmente è indispensabile effettuare un bilanciamento fra tutti gli interessi potenzialmente rilevanti

nella fattispecie. Non solo. Spesso le difficoltà aumentano per la necessità di affiancare all'esercizio della discrezionalità amministrativa anche complesse valutazioni, che possono configurarsi (applicando, in modo forse un po' semplicistico, le categorie tradizionali) come espressione di discrezionalità tecnica: si pensi, per esempio, alla distinzione tra mero dato sanitario e dato inerente allo stato di salute, che solo in parte si sovrappongono e richiedono in realtà diverse intensità di cautela nel trattamento.

Come già si è avvertito, è essenziale che le pubbliche amministrazioni, in questo intricato contesto, sappiano predisporre e mantenere le condizioni ottimali affinché il trattamento dei dati non risulti irreparabilmente pregiudizievole per il loro titolare, in particolare se si tratta di un privato poco attrezzato e vulnerabile dinanzi al potere del mercato. Gli sforzi congiunti del legislatore (*rectius*, dei legislatori), dei soggetti pubblici coinvolti nel trattamento dei dati (autorità impegnate nell'amministrazione attiva, Garanti), della giurisprudenza e della dottrina devono essere rivolti ad evitare, da un lato, semplificazioni eccessive suscettibili di sfociare nel semplicismo e, dall'altro lato, complessità talmente elevate da sfociare nella complicazione. Il problema della legalità, in particolare, può essere adeguatamente risolto solo tenendo ben distinti il piano delle norme puntuali (che si intersecano, spesso si affastellano e a tratti addirittura si contraddicono) e il piano dei principi, in cui vanno ricercate le risposte ai numerosi interrogativi applicativi aperti. Spicca per la sua portata al contempo sistematica e operativa il principio di trasparenza nella sua accezione più profonda, che richiede la piena valorizzazione dell'attività di comunicazione pubblica. Inoltre, anche in assenza di norme puntuali e specifiche in tal senso, vanno costantemente presidiati i principi di ragionevolezza, proporzionalità, leale collaborazione fra livelli istituzionali e buona fede nei rapporti con la cittadinanza. Nel settore del trattamento dei dati, poi, assume particolare rilevanza l'intreccio fra efficienza dell'organizzazione e dell'attività amministrativa, che solo congiuntamente possono offrire soluzioni efficaci a problemi complessi.

Studi e ricerche

Sistemi e applicazioni

Note e discussioni

RIVISTA ITALIANA
DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0234 • articolo sottoposto a peer review • pubblicato in anteprima il 1 ago. 2025

Giovanni Barozzi Reggiani

La *race for the cyberspace* degli Stati e il tema della cybersicurezza: tra sovranità e modelli di governance

Il contributo intende compiere una riflessione concernente il tema della dialettica tra forme di *governance* e tradizionali strumenti di *government* attraverso l'angolo di osservazione della proiezione della sovranità degli Stati sul cyberspazio e delle questioni che afferiscono (in via diretta o indiretta) alla cybersicurezza. Dalla disamina e dal raffronto dei quadri giuridici europeo e nazionale in materia, e dall'esame delle caratteristiche delle "architetture" e degli assetti organizzativi che tali quadri giudici disegnano, emerge una rinnovata centralità della sovranità, elemento caratterizzante il Leviatano hobbesiano, e dunque lo Stato nazionale, il quale, pur dovendosi oggi confrontare con le sfide complesse (e in parte inedite) che le peculiarità del cyberspazio (e le esigenze connesse agli obiettivi di cybersicurezza) pongono allo stesso, appare, nel perseguimento delle sue finalità di fondo (garantire la propria sicurezza e il proprio funzionamento e salvaguardare diritti e libertà fondamentali) tutt'altro che in crisi, ed anzi pervaso da una rinvigorita vitalità.

Cybersicurezza – Sovranità – Cyberspazio – Governance – Government

Cybersecurity in the context of the race for the cyberspace: reflections on state sovereignty in the digital world

The paper aims to investigate the relationship between governance and government in connection with the ongoing race for the cyberspace, driven by nation-states, and the issues related to cybersecurity. Starting with an overview of both the European and the Italian legal frameworks, the paper will focus on the centrality of state sovereignty in the global context. Due to the unique characteristics of the cyberspace, states today face significant challenges in protecting citizen's fundamental rights and freedoms from threats emerging from the digital realm. These challenges compel states to cooperate and develop innovative solutions. At the same time, they highlight that the traditional concept of sovereignty is not in crisis, but is instead increasingly central to the network of geopolitical relationships between States and the governance of cyberspace.

Cybersecurity – Sovereignty – Cyberspace – Governance – Government

L'Autore è ricercatore di Diritto costituzionale e pubblico presso il Dipartimento di Giurisprudenza dell'Università di Sassari

Questo contributo è stato elaborato nell'ambito del progetto di ricerca *Il ruolo della governance nei processi decisionali delle democrazie pluralistiche*, finanziato ai sensi del bando Progetti di ricerca interdisciplinare - d.m. 737/2021, risorse 2021-2022

Sommario: 1. Considerazioni introduttive. – 2. Le caratteristiche del cyberspazio (luogo fisico e virtuale) e le questioni afferenti alla costruzione di architetture di cybersicurezza. – 3. I quadri giuridico-normativi in materia di cybersecurity degli ordinamenti europeo e italiano. – 4. Osservazioni conclusive.

1. Considerazioni introduttive

Come è stato osservato, non è dato rinvenire alcuna "porzione di terra emersa che non appartenga al territorio di un'entità statale" (se si esclude l'Antartide)[1].

La sovranità degli Stati[2] – che si riferisce ai territori – si estende poi anche a talune zone marine (il c.d. mare territoriale) e allo spazio aereo sovrastante i territori medesimi (quantomeno fino a una certa altitudine); altre "porzioni di globo", che non cadono sotto la sovranità di alcun ordinamento statuale (si pensi alle acque internazionali), sono invece assoggettate a regole, di matrice prevalentemente convenzionale, che ne disciplinano la natura giuridica e il modo in cui gli ordinamenti si rapportano ad esse.

La descritta situazione risponde a quello che potremmo definire "principio dell'*horror vacui* geopolitico", compendiabile nella massima secondo cui se esiste uno spazio occupabile, prima o poi il medesimo verrà effettivamente occupato, fisicamente o "giuridicamente".

La propensione alla "occupazione di territorio", del resto, da sempre caratterizza gli Stati, in quanto espressione di quella volontà di potenza che, secondo i postulati del c.d. realismo geopolitico, spinge i medesimi a tentare di aumentare costantemente la propria influenza sullo scacchiere mondiale, e che risulta pienamente "coerente con le concezioni classiche del diritto pubblico statale, evocando l'idea dello Stato come entità sovrana autofondata e *superiorem non recognoscens*"[3], costituendo dunque un atto materiale – cui si riconnettono tuttavia

1. Così Chessa 2019, p. 12.
2. Non è certo questa la sede per disquisire sul concetto di sovranità; ciò che maggiormente interessa è chiarire quale sia l'accezione nella quale, nel presente scritto, detto termine verrà utilizzato. In questo senso, sovranità verrà qui intesa e usata come sostanziale sinonimo del concetto di *government*. Quest'ultimo, a sua volta, verrà considerato in una precisa declinazione, ovvero come riferito ai modelli di regolazione e governo di specifici fenomeni delineati dagli architravi costituzionali dei diversi ordinamenti, e quindi (e proprio per ciò, ancorché con un'opera di semplificazione) quale sostanziale sinonimo di sovranità, o comunque termine a quest'ultima riconducibile in quanto espressione della stessa. Trattasi di utilizzo del termine che, ancorché con le menzionate semplificazioni, appare ammissibile, ai fini del presente lavoro; nello stesso volume di Chessa 2019 si rinvengono espressioni che sembrano confermare la "legittimità" di detto utilizzo, laddove l'Autore parla di *government* come di "potere rappresentativo lato sensu […] che ricomprende l'intero apparato degli organi costituzionali, lo Stato-persona (o Stato soggetto, Stato-governo, Stato-apparato)" (p. 325) ovvero di "dispositivi tradizionali di government statale" (p. 336) o ancora utilizza uno accanto all'altro i termini government e sovranità statale (p. 332).
3. In questo senso Chessa 2025, p. 86.

anche effetti giuridici[4] – che esprime concretamente la sovranità.

In questo senso, ancorché si discuta da tempo (secoli, invero) circa l'ampiezza del novero delle potestà pubbliche riconducibili alla sovranità (senza che si sia addivenuti ad una sistematizzazione condivisa[5]), è difficilmente revocabile in dubbio che a quest'ultima afferisca quella che Jean Bodin definiva attività di "dichiarare la guerra e concludere la pace", che consiste (anche) nell'occupazione di territori[6].

Si tratta, peraltro, di aspirazione e prerogativa tutt'altro che "dormiente": come è stato infatti notato, attualmente si sta assistendo ad un rinvigorirsi delle "pretese territoriali" degli Stati[7], oltre che ad una progressiva corsa al riarmo pressoché in ogni parte del globo[8].

Si potrebbe dire: nulla di nuovo; gli Stati fanno ciò che fanno da sempre, e che è nella loro natura fare. Tuttavia, nel mondo moderno alcune delle ambizioni di espansione degli Stati riguardano un "territorio" che presenta caratteristiche affatto particolari.

Stiamo parlando del cyberspazio, che è stato qualificato (a partire dai primi anni del XXI secolo) in termini di "quinto dominio" (accanto a terra, acqua, aria e spazio), oggetto in quanto tale di potenziali conquiste e – conseguentemente – conflitti tra gli Stati[9].

Questi ultimi possono, su tale "dominio", proiettare la propria volontà di potenza, che si declina quale ambizione all'occupazione di "territorio" o alla regolazione di fenomeni o condotte di soggetti o attività che per il medesimo transitano (in numero sempre crescente[10]) e, specularmente, alla difesa e alla salvaguardia di dette attività nonché

4. E difatti, come è stato osservato, quella concernente l'occupazione di terra costituisce la "decisione veramente fondamentale, creativa di nuovi ordinamenti" (così ancora Chessa 2025, p. 72).
5. Ciò risulta vero al punto che autorevolissima dottrina ha affermato come appaia "preferibile rinunciare alla ricerca di itinerari che portino a trovare le 'essenze' della sovranità, e tornare alla vecchia opinione, che questa è costituita dalle somme potestà dell'ordinamento statale" (così Giannini 1990, p. 227).
6. Bodin 1576/1964, p. 495.
7. Constatazione riportata da ultimo da Cassese 2025.
8. Nel marzo 2025 la Commissione europea ha presentato il *ReArm Europe Plan/ Readiness 2030*, che prevede investimenti nel settore della difesa e del riarmo per circa 800 miliardi di euro. Nello stesso mese, la Commissione e l'Alto Rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza hanno presentato il Libro Bianco *for European Defence Readiness 2030* (doc. JOIN(2025) 120, del 19 marzo 2025), nel quale, in uno dei diversi passaggi significativi, viene affermato: "the moment has come for Europe to re-arm. To develop the necessary capabilities and military readiness to credibly deter armed aggression and secure our own future, a massive increase in European defence spending is needed. This needs to be coordinated and directed more effectively than ever between Member States, reflecting our collective strengths and addressing the weaknesses that come from uncoordinated action".
9. La definizione del cyberspazio quale "*quinto dominio della conflittualità*" si deve a William J. Lynn III, allora vice-Segretario alla Difesa degli Stati Uniti (cfr. in particolare Lynn iii 2010, p. 97). Il riconoscimento ufficiale del cyberspazio quale quinto dominio operativo si ebbe poi all'esito del Summit NATO di Varsavia del 2016. Sul fronte dell'ordinamento nazionale, una interessante epifania normativa è rappresentata dalle modifiche che l'art. 51, comma 8, lett. e) del d.l. 17 maggio 2002, n. 50 (convertito, con modificazioni, dalla legge 15 luglio 2022, n. 91) ha apportato all'art. 88 del Codice militare (decreto legislativo 15 marzo 2010, n. 66) il cui novellato comma 1 stabilisce che "lo strumento militare è volto a consentire la permanente disponibilità di strutture di comando e controllo di Forza armata e interforze, facilmente integrabili in complessi multinazionali, e di unità terrestri, navali, aeree, cibernetiche e aero-spaziali di intervento rapido, preposte alla difesa del territorio nazionale, delle vie di comunicazione marittime e aeree, delle infrastrutture spaziali e dello spazio cibernetico in ambito militare; è finalizzato, altresì, alla partecipazione a missioni anche multinazionali per interventi a supporto della pace".
10. In effetti, come è stato condivisibilmente sostenuto, a seguito del progressivo affermarsi della società dell'informazione, il cyberspazio è "diventato un elemento cruciale per le dinamiche politiche, sociali, finanziarie e umane del XXI secolo" (così Martino 2018, p. 62).

delle strutture che sorreggono il cyberspazio e ne garantiscono il funzionamento.

In effetti, è in corso una vera e propria "*race for the cyberspace*", che ha una proiezione tanto attivo-offensiva (concernente la conquista di sempre maggiori "spazi" e "territori") che passivo-difensiva (relativa alla protezione di componenti, dati, strutture) e che non appare confinata solo alla dimensione economica e commerciale dei rapporti tra gli Stati: in questo senso, costituisce un dato ormai acquisito che nel cyberspazio possono venir condotte anche operazioni militari[11], e che anzi all'attualità non è dato rinvenire un'operazione di tale natura (condotta secondo le metodologie tradizionali e in uno degli altri "dominii") che non sia preceduta o accompagnata da attività di *cyberwarfare*[12].

Come appare evidente, rispetto al quadro descritto vengono in rilievo esigenze che attengono alla stessa sicurezza dello Stato – sia sul fronte interno che su quello esterno[13] – e in specie all'interesse di quest'ultimo alla "propria integrità territoriale, indipendenza e – al limite – alla stessa sua sopravvivenza", interesse che risulta "preminente su ogni altro in tutti gli ordinamenti statali, quale ne sia il regime politico"[14].

Rispetto alla descritta prospettiva, appare certo da condividersi l'osservazione secondo la quale "l'insicurezza del cyberspazio non minaccia solo l'economia, ma addirittura il funzionamento delle nostre democrazie e i valori su cui si fonda la società [dato che] le politiche interne degli Stati che riguardano l'ordine pubblico, la sicurezza nazionale e la stessa protezione delle libertà devono fare i conti con le minacce che provengono o si consumano nel cyberspazio"[15].

Se la garanzia della sicurezza dello Stato è funzionale (anche) alla salvaguardia del

11. Emblematica in questo senso l'affermazione concernente l'invocabilità dell'art. 5 del Trattato NATO (relativo alla reciproca difesa, da parte dei membri dell'alleanza) anche in riferimento agli attacchi cibernetici (in tema cfr., da ultimo, le conclusioni della riunione dei Capi di Stato e di Governo tenuta a Vilnius l'11 luglio 2023, par. 66).
12. Particolarmente indicativo, sul punto, quanto si legge nel citato Libro Bianco *for European Defence Readiness* (al par. 8), circa il fatto che "both defensive and offensive cyber capabilities are needed to ensure the protection and freedom of manoeuvre in cyberspace. There is a need to develop together with Member States a voluntary support scheme for offensive cyber capabilities as credible deterrence". In tema, v. anche quanto osservato da De Felice 2012, p. 76, circa il fatto che "l'ampia gamma di azioni ostili può andare dallo spionaggio agli attacchi veri e propri, con finalità ibride, all'alterare o addirittura distruggere dati, hardware, reti o eventuali servizi e sistemi ad essi connessi. Generalmente possono essere rivolte ad assetti governativi, economico-finanziari, imprese, infrastrutture critiche o servizi dedicati alla società civile. I possibili effetti da essi generati possono facilmente divenire strategicamente rilevanti oppure influenzare comportamenti, azioni e documentazione collegati anche ad operazioni militari in corso".
13. Come è stato rilevato, "diversamente dal concetto di sicurezza 'reale', la cybersicurezza pone particolare rilevanza non solo verso il profilo esterno, ma anche verso quello della gestione del rischio endogeno che, nel caso specifico, ricomprende gli incidenti di sicurezza dovuti a condotte dolose di soggetti interni ad amministrazioni, organi dello Stato o dipendenti di organizzazioni private, perpetrate con o senza l'ausilio di strumenti informatici; e gli eventi riconducibili al c.d. fattore umano, ossia incidenti dovuti alla mera inconsapevolezza degli utenti circa il rispetto di buone pratiche di sicurezza informatica (best practices) o sulle tecniche di prevenzione da attacchi di ingegneria sociale" (così Serini 2022, p. 271).
14. Sentenza n. 82 del 1976, punto 5 Cons. in Dir. Nello stesso senso si sono espresse le sentenze n. 86 del 1977 (punto 5 Cons. in Dir.); n. 106 del 2009 (punto 3 Cons. in Dir.); n. 40 2012 (punto 4 Cons. in Dir.); n. 24 del 2014 (punto 5 Cons. in Dir.).
15. Longo 2024-a, p. 314. In senso analogo cfr. Pietrangelo 2024, p. 17, la quale osserva che "nelle politiche e pratiche della transizione digitale la cybersicurezza è oggettivamente una condizione di esistenza: rendere più sicuri reti, sistemi e dati vuole dire giocoforza rendere più sicuri gli Stati e i loro apparati, le persone e le loro vite. Una specie di protezione delle protezioni, una sicurezza maxima da cui dipendono le sorti delle Nazioni come degli individui, tutti inesorabilmente immersi nella dimensione digitale". Il concetto in esame mi pare peraltro

funzionamento delle democrazie, e più ampiamente dell'ordinamento costituzionale, e se il cyberspazio è un dominio nell'ambito del quale tale sicurezza può venir messa in discussione, ne consegue, per semplice sillogismo, che gli Stati devono farsi carico di garantire specifiche istanze di sicurezza concernenti il cyberspazio anche nell'ottica di salvaguardare i diritti e le libertà fondamentali degli individui (che vengono garantiti dall'ordinamento costituzionale ed anzi, come autorevolmente sostenuto, sono la causa e il fondamento delle Costituzioni[16]).

L'obiettivo della protezione di diritti e libertà amplia peraltro l'ambito di operatività delle istanze difensive e di sicurezza che riguardano il cyberspace; detti diritti e libertà, infatti, possono venir minacciati non solo da attività ostili provenienti da altre entità statuali o da gruppi terroristici, ma anche da soggetti che svolgono nello spazio virtuale attività illecite (come il furto dei dati o le truffe)[17] o semplicemente dalla commissione, anche in buona fede o per semplice ingenuità, di errori.

In questo senso, dalla cyber-difesa (attività, di natura prevalentemente militare, che concerne principalmente il tema del contrasto al *cyberwarfare*, e quindi delle azioni ostili provenienti da Stati o comunque agli stessi riconducibili) si passa al più ampio concetto di cybersicurezza, del quale si rinvengono anche definizioni normative, tra cui quella posta dal Regolamento (UE) 2019/881[18], che definisce il termine quale "insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche", o quella che si rinviene nel d.l. n. 82 del 2021, il cui art. 1, al comma 1, lett. a), descrive il concetto come "l'insieme delle attività, fermi restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124, e gli obblighi derivanti da trattati internazionali, necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico"[19].

Da entrambe le definizioni – con la seconda che chiaramente rende l'idea della complementarietà tra cybersicurezza e attività di *intelligence* – emerge l'immagine della cybersicurezza quale complesso di

ben reso dalla definizione di "resilienza nazionale nello spazio cibernetico", posta dall'art. 1, comma 1, lett. b) del d.l. 14 giugno 2021, n. 82 – che ha tra le altre cose istituito e disciplinato l'Agenzia Nazionale (italiana) per la Cybersicurezza – che qualifica il concetto come l'insieme delle "attività volte a prevenire un pregiudizio per la sicurezza nazionale" che possa comportare un "danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici militari, economici scientifici e industriali dell'Italia, conseguentemente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale […]".

16. Quella così sintetizzata (e si spera non banalizzata) è la tesi di fondo del lavoro di Chessa 2002.
17. La strumentalità della messa in sicurezza del *cyberspace* a garantire diritti e libertà fondamentali dei singoli è sottolineata anche dalla Direttiva del 1° agosto 2015 della Presidenza del Consiglio dei Ministri (che ha imposto alle pubbliche amministrazioni l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici). Come è stato sottolineato, "si tratta di un passaggio di grande significato politico, ma anche giuridico: viene riconosciuto che il tema della cyber security non è solo questione di 'difesa nazionale', ma è di garanzia per i diritti fondamentali degli individui, quelli, cioè, costituzionalmente protetti" (così Bruno 2020, p. 16).
18. Regolamento (UE) 2019/881 del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013.
19. È un concetto, quello del rapporto tra attività di cyber-difesa e attività di cyber-sicurezza, che si rinviene ben compendiato nella *Indagine conoscitiva sulla difesa cibernetica: nuovi profili e criticità* della IV Commissione permanente del Senato (di cui il 2 aprile 2025 è stato approvato il documento conclusivo) laddove si legge (p. 75) che "la difesa cibernetica si sostanzia in uno spettro di competenze dello Stato di natura prettamente militare, da inquadrare in una più ampia strategia nazionale per la sicurezza cibernetica, la cui architettura si è andata componendo grazie a una serie di interventi normativi".

attività (che dunque costituiscono un insieme, non necessariamente omogeneo[20]) strumentali alla protezione di alcuni beni – che sussistono o trovano inedite modalità di estrinsecazione nel cyberspazio – da "minacce informatiche", concetto, quest'ultimo, che ha un notevole ambito di estensione, essendo stato definito (sempre dal Regolamento europeo 2019/881) come "qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone" (art. 2, punto 8).

Le minacce informatiche[21], se efficacemente attuate, possono poi determinare il verificarsi di un incidente, come tale qualificato – in particolare dall'art. 6, n. 6, della Direttiva (UE) 2022/2555 (c.d. Direttiva NIS II[22], che ha abrogato la Direttiva (UE) 2016/1148, c.d. NIS I) – qualsiasi "evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi"[23].

Sono dunque tali minacce, e per esse gli incidenti informatici, a costituire il fattore cui le attività di cybersicurezza (e di *cyber-defence*) devono prestare la principale attenzione, posto che è da tali attività che può derivare la reale lesione o anche solo la semplice messa in pericolo dei beni giuridici e degli interessi alla cui salvaguardia la cybersicurezza è preposta[24].

Tale conclusione pone il tema di come tali minacce possano venire efficacemente contrastate.

Nell'ottica di fornire risposta al quesito – e prima di interrogarci su quali siano i "modelli regolatori" più adatti allo scopo (specie a riguardo della dialettica *governance* – *government*[25])

20. Al concetto di cybersicurezza, secondo le definizioni richiamate, sarebbe riconducibile un triplice ordine di attività: "da un lato la protezione dei contenuti, dei dati, delle informazioni, un secondo relativo alla protezione hardware (quindi gli elementi fisici dei dispositivi quali PC, Smartphone, Mainframe, Server ecc.); una terza protezione relativa agli aspetti software intesi quali programmi, reti, database, archivi digitali ed altre impostazioni tecnologiche militari" (così Contaldo–Salandri 2020, p. 2).
21. Per un inquadramento delle principali minacce informatiche v., nel sito ENISA, *Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride!*
22. Il termine "NIS" è acronimo di *Network and Information Security*.
23. Anche rispetto alla definizione in parola si evidenzia il focus peculiare sui dati, specie se tale definizione viene raffrontata a quella posta dalla Direttiva NIS I, che definiva l'incidente (all'art. 4, n. 7) come "ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi" (senza quindi un esplicito riferimento ai dati). La Direttiva NIS II contiene peraltro una definizione anche del concetto di "incidente di cibersicurezza su vasta scala", definito quale "incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un impatto significativo su almeno due Stati membri" (art. 6, n. 7).
24. Si tratta di insieme di beni e interessi ad ampio spettro, che comprende tanto interessi strategici dello Stato quanto "l'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" (così Longo 2024-b, p. 67).
25. Il tema del rapporto tra *government* e *governance* ha fatto versare alla dottrina i proverbiali fiumi di inchiostro. Per una bibliografia minima si rimanda a quella riportata da Chessa 2019, p. 331, nt. 15 (oltre che alle osservazioni dello stesso Chessa al Capitolo Quindicesimo della sua corposa monografia). Ai fini del presente scritto, e rinviando a quanto esposto in precedenza sul *government* (cfr. nt. 2), si rileva che del concetto di *governance* non si rinviene una definizione condivisa. In dottrina, è stato affermato che detto termine "signifies a change in the meaning of government, referring to a new process of governing; or a changed condition of ordered rule; or the new method by which society is governed" (così Rhodes 1996, p. 653) ovvero che il medesimo indica "un nuovo stile di governo, distinto dal modello del controllo gerarchico e caratterizzato da un maggior grado di cooperazione e dall'interazione tra lo Stato e attori non-statuali all'interno di reti decisionali miste pubblico/private" (così Mayntz 1999, p. s.). La *governance* concernerebbe dunque un modo di governare, e quindi regolare, un determinato fenomeno, ma secondo schemi e modalità diversi da quelli riferibili al *government*; più nello specifico, come è stato osservato, entrambi i termini "refer to purposive behavior, to goal oriented

– appare indispensabile effettuare qualche considerazione sulla natura e sulle caratteristiche del cyberspazio, che configura un luogo (un territorio, un dominio) diverso da tutti gli altri, e che proprio in ragione di tale diversità richiede di declinare in senso particolare l'ambizione all'occupazione di territorio e la volontà di potenza degli Stati.

2. Le caratteristiche del cyberspazio (luogo fisico e virtuale) e le questioni afferenti alla costruzione di architetture di cybersicurezza

È noto che la coniatura del termine "cyberspazio" si deve ad uno scrittore di fantascienza, William Gibson, che lo utilizzò dapprima nel racconto *Burning Chrome*, pubblicato nel 1982, e successivamente nel romanzo *Neuromante* (che ha visto le stampe nel 1984), considerato una delle pietre miliari del genere letterario *cyberpunk*.

Se il termine è divenuto ormai di largo utilizzo, non vi è però certezza e condivisione sul suo esatto significato.

Nel *Glossario* della *Guide for Conducting Risk Assessments* redatta dal *National Institute of Standards and Technology* del *Department of Commerce* statunitense, il cyberspazio è definito come "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers"[26].

Si tratta, invero, di una definizione che non può oggi considerarsi pienamente appagante ed esaustiva, nella misura in cui pone un'eccessiva (ed anzi esclusiva) enfasi sugli elementi "fisici" che connotato il cyberspazio, il quale è invece caratterizzato dal fatto che "alla sua formazione concorrono sia elementi naturali che virtuali"[27].

---

activities, to system of rule; but government suggests activities that are backed by formal authority, by police powers to ensure the implementation of duly constituted policies whereas governance refers to activities backed by shared goals that may or may not derive from legal and formally prescribed responsibilities and that do not necessarily rely on police powers to overcome defiance and attain compliance" (così Rosenau–Czempiel 1992, p. 4, i quali aggiungono poi che il concetto di *governance* "embraces governamental institutions but it also subsumes informal, non-governamental mechanisms whereby those persons and organizations within its purview move ahead, satisfy their needs and fulfill their wants"). Nei modelli di *governance*, in particolare, l'elemento della decisione autoritativa risulterebbe più affievolito, venendo in rilievo un modo di governare i fenomeni e assumere decisioni di carattere più "orizzontale e diffuso" che "verticale e decifrabile" (il quale ultimo caratterizza invece – cfr. D'Orsogna 2024, pp. 923 ss., nt. 83 – i modelli di *government*), cui prenderebbe parte una pluralità di attori e nel quale un ruolo di primo rilievo verrebbero a giocare soggetti dotati di particolare *expertise* tecnica, nella logica dell'effettuazione di scelte regolatorie basate su criteri obiettivi (in quanto aventi matrice tecnico-scientifica) che si imporrebbero (anche al decisore politico) proprio in ragione della loro "oggettività". A fronte di ciò, resta il tema della difficile inquadrabilità del concetto di *governance*; osserva in questo senso Barletta 2019, che il termine sarebbe suscettibile di "ricomprendere ipotesi di governo complesso nel quale interagiscono diversi attori con differenti provenienze istituzionali", venendo utilizzato in svariate accezioni, che vanno "da governance intesa come processo sino a governance intesa come governo della cosa pubblica o gestione di società commerciali". Ciò detto, si osserva che l'affermazione di modelli di *governance* a scapito della tradizionale rappresentanza/decisione politica sarebbe da ascriversi alla ormai acclarata incapacità del *government* di intercettare e regolare efficacemente diversi fenomeni della contemporaneità e di rispondere a istanze sociali (in tema, tra gli altri, Negri 2011, p. 206) e produrrebbe la conseguenza che "in ambiti sempre più vasti non c'è più la deliberazione politica degli organi rappresentativi e di governo, non c'è più la scelta unilaterale di indirizzo politico e la sua immediata traduzione in atti normativi e attività amministrative, secondo i tradizionali moduli gerarchici" dato che "alla direzione politica si sostituiscono la valutazione tecnica e l'accordo informale guidato da criteri che si rappresentano come scientificamente obiettivi e quindi a-politici" (Chessa 2019, p. 333).

26. National Institute of Standards and Technology – U.S. Department of Commerce, *Guide for Conducting Risk Assessments*, Special Publication 800-30, September 2012, p. B-3.

27. Martino 2018, p. 64.

In questo senso, appaiono più corrette definizioni come quella proposta da Ottis e Lorents, secondo la quale "cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems"[28], o quella avanzata da Khuel, che ne parla in termini di "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies"[29].

La rilevanza (e la "maggior correttezza") di definizioni come quelle da ultimo richiamate è data dalla loro idoneità a dare conto del carattere polistrutturato e polimorfo del cyberspazio, che è composto da elementi materiali e immateriali, strutture, software ma, anche, esseri umani, che si muovono e agiscono al suo interno contribuendo, mediante i dati e le informazioni che fanno circolare e rendono disponibili, a farlo crescere e funzionare.

Ed invero, secondo le ricostruzioni più comuni e accettate il cyberspazio si strutturerebbe su tre distinti (ma interconnessi) *layers*, denominati "fisico", "logico" e "sociale"[30].

Sul piano "fisico" si collocherebbero le infrastrutture e, in generale, le componenti hardware indispensabili a consentire la circolazione dei dati (cavi sottomarini, antenne, computer, e così via[31]).

Il piano "logico" è invece quello nel quale si rinvengono i software e i codici che consentono a macchine (gli hardware) di dialogare tra loro, definendo le regole del funzionamento del cyberspazio[32].

Infine, il piano sociale (detto anche della "*cyber-persona*") è formato dalle interazioni che possono verificarsi fra persone fisiche o, come ormai sempre più spesso accade, tra persone e macchine o tra macchine e macchine.

Considerate le descritte caratteristiche, è certo da accogliere la posizione di chi si riferisce al cyberspazio come a un concetto atto a "identificare un'area/spazio (virtuale) in cui coesistono e funzionano in modo coordinato reti di computer, web semantico, social media e altre tecnologie dell'informazione e della comunicazione (ICT)"[33], e in cui operano persone; tali "componenti" (persone incluse) "risiedono, simultaneamente, nello spazio fisico e nello spazio virtuale, così come all'interno e all'esterno dei confini geografici"[34].

La base del cyberspazio è dunque certo fisica (esso funziona su e per il tramite di strutture o elementi reali e aventi una concreta dimensione nella realtà), ma il medesimo configura un luogo, o un insieme di luoghi, che, a differenza di tutti gli altri, prescinde dal requisito della territorialità[35], oltre a non avere una sua struttura fissa e definita, essendo dinamico (in quanto basato sulle continue relazioni

28. Ottis–Lorents 2010, p. 268.

29. Khuel 2009, p. 28.

30. In alcuni lavori, si rinviene una terminologia parzialmente diversa, senza che si riscontrino però sostanziali differenze circa il contenuto dei termini. Si veda ad esempio Libicki 2009, p. 12 ss., che parla di livelli fisico, sintattico e semantico.

31. Secondo alcuni Autori, il *layer* "fisico" sarebbe scomponibile in due sotto-livelli, quello geografico e quello fisico-infrastrutturale; in tema, tra gli altri, v. Pătrașcu 2019, p. 53, il quale rileva che "the geographic component has the role of hosting cyber infrastructures in its specific environments (soil, water, air and space), while the physical network component is made up of cyber infrastructures that are supported by connectors for the physical network which are a combination of wired and wireless links and satellites".

32. Sul punto è stato osservato che "the logical layer is where cyber terrain exists, and the primary cyberspace terrain feature is the network, a collection of devices that implement applications, services, and data stores" (così McCroskey–Mock 2017, p. 44).

33. Matassa 2023, p. 25.

34. Ursi 2023, p. 8.

35. In questo senso, se è vero che "the physical layer is the hardware, located in the physical domain, on which the other two layers exist" il medesimo "is not cyberspace terrain itself" (McCroskey–Mock 2017, p. 44).

che gli utenti instaurano tra loro) e pertanto definibile in termini di "spazio-movimento"[36].

Da tali caratteristiche discende la "irrelevance of geographic boundaries", dal momento che "cyberspace is about cross-border electronic communications"[37], costituendo un "virtual medium, one far less tangible than ground, water, air, or even space and the RF spectrum"[38].

Piuttosto, l'elemento che si configura come realmente costitutivo e caratterizzante il cyberspazio (o quantomeno essenziale per il suo funzionamento) è rappresentato dai dati[39].

La centralità di questi ultimi per il funzionamento del cyberspazio (ed anzi per la comprensione della natura profonda dello stesso) emerge in modo chiaro in alcune delle più recenti definizioni (sempre di cyberspazio)[40].

Negli anni, la mole di dati che circolano nel *cyberspace* è cresciuta esponenzialmente e, con essa, il numero di attività – fondate sui dati o aventi questi ultimi quale oggetto specifico – che nel medesimo vengono svolte; le applicazioni dell'intelligenza artificiale, divenute sempre più efficienti e precise grazie alla raffinazione dei processi di *machine learning* e il ricorso ai c.d. *big data*, hanno offerto una gamma via via maggiore di servizi, con la conseguenza che all'attualità il cyberspazio costituisce un luogo nel quale vengono svolte molte delle attività che caratterizzano la quotidianità (economica e sociale) dei singoli[41], comprese alcune riconducibili a servizi essenziali (aventi, in quanto tali, un rilievo pubblicistico) o a prestazioni rese dalle pubbliche amministrazioni, sempre più digitalizzate e in grado di dialogare con i cittadini/utenti mediante modalità telematiche e digitali (SPID, carta d'identità elettronica, e così via).

Ne consegue che le istanze concernenti la protezione dei dati e delle modalità con le quali i medesimi circolano assumono un primario rilievo, a riguardo della cybersicurezza e del contrasto alle minacce informatiche[42].

36. "Chi si avventura nel cyberspace vaga senza fine tra reti di comunicazione, inventando nuovi spazi e nuove velocità. È per così dire inafferrabile, giacché il suo spazio non è mai strutturato a priori, non è fisico, bensì dinamico, è cioè spazio-movimento" (così Amato Mangiameli 2000, p. 7).
37. Così Longworth 2000, p. 14.
38. Libicki 2009, p. 12.
39. Ed infatti, il cyberspazio configura una realtà "fatta di 'cose' che si vedono e si sentono, ma che non sono oggetti fisici né, necessariamente, rappresentazioni di oggetti fisici, bensì costrutti di dati" (così Tagliagambe 1997, p. 39). È stato in questo senso altresì osservato che "la produzione, l'immagazzinamento, la diffusione dei dati sono i motivi principali che spingono allo sviluppo del cyberspace" (così Mirti 2021, p. 42).
40. Si veda in questo senso quella che si rinviene nel *Glossary of Terms and Definitions* NATO (AAP-06 Edition 2018), che lo qualifica come "the global domain consisting of all interconnected communication, information technology, and other electronic systems, networks, and their data, including those which are separated or independent, which process, store, or transmit data". In termini analoghi si esprimono le Linee Guida ISO/IEC 2018, che definiscono il cyberspace come un "complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form".
41. È in questo senso stato correttamente rilevato che "cyberspace is where we create and use the digital information that fuels the global economy. Every day, the global business community exchanges trillions of dollars via cyberspace, transactions in which not a single dime or euro of hard currency is moved" (così Khuel 2009, p. 29).
42. Alla cybersicurezza può dunque ricondursi il tema della protezione dei dati degli individui (o delle imprese o delle amministrazioni) rispetto a tentativi di furto, appropriazione o danneggiamento da parte dei terzi: del resto, alcune delle tradizionali minacce informatiche (si pensi al *phishing*) hanno proprio ad oggetto la sottrazione di dati; tuttavia, le connessioni tra cybersicurezza e tutela dei dati personali (disciplina che concerne specificamente le modalità di trattamento, conservazione ed eventuale diffusione o comunicazione degli stessi, anche per fini economico-commerciali) non si esauriscono a temi legati al contrasto a episodi di *data breach* o altri fenomeni di furto o sottrazione dei dati. Nell'impossibilità di approfondire in questa sede tali connessioni si rinvia, sul tema, a Ponti 2024, p. 58 ss. Più ampiamente sul tema della regolazione dei dati nell'ambito della

Da ultimo, deve darsi conto di un ulteriore fattore caratterizzante il cyberspazio, rappresentato dal fatto che nessuna delle componenti del medesimo costituisce una monade isolata e indipendente, configurando piuttosto una parte del tutto (a questo, e alle altre componenti dello stesso, connessa)[43].

Una caratteristica, quella della interconnessione/interdipendenza – che emerge anche da alcune definizioni di cyberspazio contenute in documenti diffusi a livello internazionale[44] – che si traduce nell'idea secondo la quale la garanzia dell'integrità e della capacità di operare correttamente ed efficientemente delle singole componenti del cyberspazio può configurare un elemento atto ad assicurare il funzionamento e la sicurezza del medesimo (complessivamente inteso): come è stato infatti osservato, in certe circostanze anche una piccola vulnerabilità dei sistemi informativi, delle reti o dei dati può determinare incidenti e danni a parti più o meno vaste del cyberspazio[45].

Ne discende, da un lato, che le singole componenti di quest'ultimo, o quantomeno alcune di esse, nella prospettiva della cybersicurezza assumono una rilevanza e un valore che risulta molto maggiore di quello che esse avrebbero se considerate isolatamente e in sé; dall'altro, che gli Stati non possono limitarsi a garantire e proteggere esclusivamente quelle componenti che cadono sotto il proprio dominio (la propria sovranità), dovendosi preoccupare anche delle scelte e delle condotte degli altri Stati.

Ne dovrebbe conseguire una "comune e globale" tensione di tutti gli Stati verso il conseguimento dell'obiettivo del raggiungimento di un elevato livello di sicurezza dei sistemi informatici e di rete, dei dati e in generale delle componenti che regolano il funzionamento del cyberspazio.

Le cose, tuttavia, non stanno sempre in questi termini, e talvolta la realtà offre scenari ben diversi.

Ciò si deve al fatto che alcuni Stati possono non aver alcun desiderio di garantire la sicurezza e il buon funzionamento delle strutture che si collocano nell'ambito della sfera della propria sovranità, o potrebbero addirittura voler sfruttare tale circostanza per ottenere vantaggi sul piano geopolitico e delle relazioni internazionali.

A ciò aggiungasi che alcuni Stati, ancorché "volenterosi", potrebbero non essere in grado di garantire adeguati livelli di cybersicurezza per carenza di risorse o di capacità tecniche.

Ecco perché pensare che possa conseguirsi un adeguato livello di sicurezza del cyberspazio (e di una o più delle attività che nel medesimo vengono svolte) mediante le attività di cybersicurezza o cyberdifesa che gli Stati *spontaneamente*, vale a dire in assenza di obblighi vincolanti, pongono in essere, rappresenta un'illusione, e dunque un presupposto errato da cui muovere.

Occorre piuttosto ragionare di una regolazione del cyberspazio[46] (e della costruzione di

società digitale v. Iannuzzi 2024, p. 107 ss.; Calzolaio 2023, p. 13 ss.; Colapietro 2023, p. 151 ss.; Colapietro 2021, p. 831 ss.

43. Sul tema del rapporto tra interconnessione e sicurezza (del cyberspazio) v. Djurdjevic–Stevanovic 2016, p. 15 ss.
44. Si veda ad esempio quella che si rinviene nel Volume 2 del documento NISTIR 8074, redatto dall'*International Cybersecurity Standardization Working Group del National Security Council's Cyber Interagency Policy Committee* statunitense, che lo descrive come un "complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it" (International Cybersecurity Standardization Working Group of the National Security Council's Cyber Interagency Policy Committee, NISTIR 8074, Volume 2, *Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*, December, 2015).
45. Salvaggio 2023, p. 140: "Although the application of adequate software engineering processes can reduce the probability of exploitable weaknesses and mitigate their severity, even a small mistake on the part of one of the many members of a developing chain can remain unnoticed for long while fully compromising the security of the systems overall".
46. Abbandonando così definitivamente l'approccio basato sulla affermata necessità di "lasciare libera" la rete, approccio i cui principi ispiratori sono compendiati nella nota *Declaration of the Independence of Cyberspace* di J.P. Barlow del 1996.

architetture organizzative e istituzionali di cybersicurezza) effettuata a mezzo degli strumenti del diritto internazionale, con la definizione di regole accettate da un numero il più possibile elevato di Stati, che contemperi le esigenze della (preservazione) della sovranità dei medesimi con quelle connesse alla cybersicurezza e alla garanzia del buon funzionamento dei sistemi e delle reti (e conseguente salvaguardia delle attività e dei diritti che tramite le stesse vengono esercitate)[47].

Non potendo in questa sede approfondire il tema di quale debba considerarsi, fra quelli proposti, il modello più efficace e realizzabile di regolazione globale del cyberspazio, ci si limiterà a ragionare sul se e su quali limitazioni alla sovranità degli Stati imponga la costruzione di architetture di cybersicurezza che prevedano obblighi specifici per gli Stati medesimi, e se tale costruzione imponga, in ragione delle caratteristiche del cyberspazio, un'erosione del *government* in favore di modelli di *governance* ovvero se il primo conservi una sua primarietà nelle questioni concernenti la cybersicurezza.

Procedendo sul tema, si osserva che ai singoli Stati potrebbe venir richiesta una limitazione di sovranità che potrebbe afferire ad esigenze di "protezione fisica" di una o più infrastrutture, ovvero l'accettazione di regole (tecniche e non) concernenti la realizzazione e il successivo mantenimento in funzione delle infrastrutture stesse o la garanzia delle attività che si svolgono nel cyberspazio.

La prima tipologia di richiesta è naturalmente difficilmente "digeribile", per gli Stati, specie laddove la medesima dovesse prevedere la presenza "sul territorio" di elementi (strutture, veicoli, tecnici o addirittura soldati) riferibili a realtà statuali straniere.

È invece più probabile che questi ultimi accettino la definizione di regole e standard concernenti il funzionamento e la sicurezza di uno o più aspetti del cyberspazio (comprese le infrastrutture)[48] ovvero di entrare a far parte di un circuito di cooperazione e gestione in qualche modo "condivisa" (anche per il mezzo di network di enti o organismi) di eventuali minacce e incidenti: si tratta indubbiamente anche in questo caso di cessioni di sovranità – sul piano della potestà legislativa, e quindi della produzione di regole, o dell'organizzazione amministrativa o di altro ancora – ma alle quali diversi Stati, in molti altri ambiti (la storia dell'ordinamento dell'Unione europea ne fornisce la più evidente conferma), hanno acconsentito.

Rispetto, dunque, al descritto profilo, appare del tutto possibile che gli Stati accettino limitazioni alla propria sovranità, limitazioni che, a ben vedere, rispondono agli interessi degli Stati stessi, i quali (unitamente al "popolo" agli stessi riferibile) oltre a poter trarre vantaggio da un cyberspazio "ben funzionante" potrebbero ottenere benefici da risorse (economiche e tecniche) loro assegnate quale contropartita all'assunzione di obblighi volti alla costruzione di un determinato modello di *governance* della cybersicurezza e a garanzia dell'efficace adempimento degli stessi.

Si è utilizzato appositamente il termine *governance* in ragione delle caratteristiche che possiedono alcuni dei modelli di architetture di cybersecurity che sono stati storicamente definiti (in particolare negli Stati Uniti d'America e nell'ordinamento dell'Unione europea), caratteristiche che *apparentemente* collocano i medesimi in una posizione distante dai tradizionali modelli di *government*.

Un'importante presenza di regole e standard a forte contenuto tecnico – elaborate nell'ambito di

47. In effetti, molte voci si sono espresse in tal senso, senza che tuttavia sia emersa una soluzione condivisa circa il modello regolatorio da considerarsi più adatto e le modalità di ripartizione degli obblighi tra i singoli Stati; come è stato infatti rilevato in dottrina, "mentre alcuni esperti, come evidenziato nello studio 'Cyber Governance: Balancing Sovereignty and Global Cooperation' (Oxford Journal of Cyber Policy, 2023), sostengono che il cyberspazio debba essere considerato un bene comune globale, altri, come riportato nel 'NATO Cyber Defence Policy Framework' (2024), enfatizzano la necessità di una regolamentazione sovrana che permetta agli stati di controllare e proteggere i propri asset digitali" (così Calabrese, 2025).

48. Come è stato osservato, "establishment and use of international cybersecurity standards are essential for: ensuring the integrity and reliable operation of critical infrastructure, improving trust in online transactions, mitigating the effects of cyber incidents (e.g., crime), and ensuring secure interoperability among trade, law enforcement, and military partners, thereby facilitating increased efficiencies in the global economy" (Nistir, Volume 2, cit., p. 2).

processi decisionali sostanzialmente cooperativi e ai quali partecipano diversi attori (statali e non) –, la prevista istituzione di Autorità e organismi a loro volta dotati di ampia *expertise*, una (almeno apparente) compressione della discrezionalità politico-amministrativa degli Stati e incentivi all'attivazione di forme di partenariato pubblico privato costituiscono elementi che sembrano ricondurre le architetture istituzionali e normative di cybersecurity che si rinvengono in alcune importanti realtà alla vasta ed eterogenea (e invero forse indefinita) costellazione dei modelli di *governance*, e che parrebbero collocare in una posizione di secondo piano i "dispositivi tradizionali di government statale"[49].

Si tratta tuttavia di una conclusione solo apparentemente corretta, come emergerà dalla disamina di uno specifico quadro normativo-istituzionale concernente la cybersicurezza (quello europeo) e dal suo raffronto con quello riconducibile ad uno Stato membro dell'Unione (l'Italia), disamina che – si ritiene – mostrerà come in materia di cybersicurezza appaia corretto parlare, più che di crisi della sovranità, di compenetrazione e complementarietà fra *governance* e *government*, con il secondo a costituire il reale fondamento della prima (alle condizioni dallo stesso poste).

3. I quadri giuridico-normativi in materia di cybersecurity degli ordinamenti europeo e italiano

In riferimento al contesto europeo (e limitando l'analisi alle iniziative e agli atti concernenti in via diretta la cybersicurezza[50]) un primo atto che può menzionarsi è la comunicazione congiunta della Commissione europea e dell'Alto Rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza del 7 febbraio 2013, dal titolo *Strategia dell'Unione europea per la cybersicurezza: un ciberspazio aperto e sicuro*[51].

In essa emergeva la consapevolezza delle istituzioni dell'Unione circa l'importanza del cyberspazio e della necessità di una sua regolazione al fine di tutelare diritti, beni e valori di sicuro rilievo per l'ordinamento europeo (quali "i diritti fondamentali, la democrazia e lo Stato di diritto") rispetto al rischio del verificarsi di "incidenti, attività dolose e abusi"[52].

Inoltre, la Strategia metteva bene in luce la pluralità di soggetti (pubblici e privati) dai quali dipendono l'organizzazione e il funzionamento del cyberspazio, pluralità che doveva venir prioritariamente considerata nella definizione dei modelli di *governance* (così espressamente denominati) di quest'ultimo[53].

49. Quella riportata è una citazione tratta dal volume di Chessa 2019.
50. Ed infatti, è opportuno precisare che le iniziative dell'Unione europea "hanno riguardato l'ambito trasversale a diverse politiche dell'Ue della sicurezza delle reti e sicurezza dell'informazione" (così Marrani 2021, p. 80). Proprio la "trasversalità" della "materia" cybersicurezza ha imposto all'Unione di prevedere, in tutti gli atti afferenti al tema, disposizioni concernenti il raccordo con altre politiche settoriali e con discipline che, regolando attività che si svolgono principalmente per il tramite della rete, intercettano direttamente o indirettamente il tema della cybersicurezza (tra cui il GDPR, il *Digital Markets Act*, il *Digital Services Act*, l'*AI Act*).
51. Doc. JOIN(2013) 1. È tuttavia opportuno precisare che il termine "cybersecurity" era comparso già nella relazione sull'implementazione della Strategia europea in materia di sicurezza del 2003, pubblicata nel 2008 (Consiglio dell'Unione europea, *Relazione sull'attuazione della strategia europea in materia di sicurezza. Garantire sicurezza in un mondo in piena evoluzione* (S407/08), 11 dicembre 2008), ma "è il 2013 a costituire l'anno spartiacque in termini di avanzamento cibernetico a livello comunitario" (Borriello–Fristachi 2022, p. 162). Per una ricostruzione di atti e politiche europee latamente riconducibili alla cybersicurezza adottate in epoca antecedente al 2013 si rimanda alla ricostruzione di Longo 2024-c, p. 209 ss.
52. Per entrambi i riferimenti v. il § *1.1. Contesto*.
53. Al § 1.2. *Principi della cibersicurezza*, si legge che "il mondo digitale non è controllato da un'entità singola: attualmente sono parecchi i soggetti interessati, tra cui entità commerciali e non governative, implicati nella gestione quotidiana delle risorse, dei protocolli e delle norme di internet e nel futuro sviluppo della rete. L'Ue ribadisce l'importanza di ciascun soggetto interessato nell'attuale modello di governance e appoggia questo approccio partecipativo alla governance di internet" e che "la crescente dipendenza dalle tecnologie dell'informazione e delle comunicazioni in tutti i campi della vita umana ha creato vulnerabilità che è necessario definire

Nel sottolineare la centralità degli Stati nella definizione delle politiche e delle azioni in materia di cybersicurezza, la *Strategia* indicava alcuni interventi specifici volti a "rafforzare l'efficienza complessiva dell'Ue" (in materia), con particolare riferimento allo sviluppo della cyber-resilienza – tesa "a contrastare i rischi e le minacce cibernetiche aventi dimensione transfrontaliera e a preparare a una risposta coordinata in situazioni di emergenza" – e della cybersicurezza (nell'Unione europea), quest'ultima intesa come funzionale ad "aumentare la resilienza dei sistemi informativi e di comunicazione che supportano gli interessi della difesa e della sicurezza nazionale degli Stati membri"; rispetto alle azioni e alle direttrici indicate, un ruolo di primario rilievo veniva attribuito all'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), che era stata istituita nel 2004[54].

Sulla Strategia il Parlamento adottò una apposita Risoluzione (il 12 settembre 2013), che – nel condividere nel complesso il contenuto della Strategia medesima e nel formulare ulteriori indicazioni e indirizzi – pose particolare enfasi sulla necessità dell'adozione (o dell'aggiornamento) di *Strategie nazionali per la cybersicurezza* da parte degli Stati membri, volte a disciplinare "gli aspetti tecnici e quelli relativi al coordinamento, alle risorse umane e alla dotazione finanziaria" e recanti "regole specifiche sui benefici e le responsabilità del settore privato, al fine di garantire la partecipazione di quest'ultimo, nonché a prevedere procedure complete per la gestione del rischio e a salvaguardare il quadro normativo" (punto 5).

L'adozione di Strategie nazionali (in materia di sicurezza delle reti e dei sistemi informativi) venne ad assumere carattere obbligatorio a fronte dell'entrata in vigore della Direttiva NIS, la quale "rappresenta la prima disciplina UE introdotta con l'intento di innalzare la protezione della rete e dei sistemi informativi degli Stati membri dell'Unione attraverso un approccio orizzontale"[55].

Oltre a rendere obbligatoria la definizione di Strategie nazionali, la Direttiva NIS definì (in un'ottica di armonizzazione) i contenuti minimi obbligatori delle Strategie, che dovevano individuare (art. 1, par. 1), oltre a obiettivi e priorità, il "quadro della governance" ("inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti") per il conseguimento degli stessi, le misure di preparazione, risposta e recupero, "inclusa la collaborazione tra settore pubblico e settore privato", programmi di formazione, sensibilizzazione e istruzione e piani di ricerca e sviluppo, oltre a un piano di valutazione dei rischi e "un elenco dei vari attori coinvolti nell'attuazione della strategia"[56].

Inoltre, la Direttiva previde (all'art. 8) l'obbligo, per gli Stati, di istituire "Autorità competenti in materia di sicurezza delle reti e dei sistemi informativi" e un "Punto di Contatto Unico in materia di sicurezza delle reti e dei sistemi informativi" (che poteva coincidere con l'Autorità), dotati (l'una e l'altro) "di risorse adeguate per svolgere in modo efficiente ed efficace i compiti loro assegnati e conseguire in questo modo gli obiettivi della […] direttiva" (così l'art. 8, al par. 5).

Gli Stati erano poi tenuti a designare "Gruppi di intervento per la sicurezza informatica in caso di incidente" (CSIRT), destinati a essere inseriti in una rete europea (art. 12), e a stilare elenchi di operatori di servizi essenziali e digitali, chiamati ad adottare una serie di misure (di prevenzione e gestione dei rischi) e a notificare all'Autorità competente o al CSIRT gli incidenti aventi un impatto rilevante sulla continuità dei servizi prestati.

Di fondamentale rilievo risultavano, altresì, i previsti obblighi di sicurezza e di notifica per gli

adeguatamente, analizzare in profondità, riparare o ridurre. Tutti gli attori implicati, siano essi autorità pubbliche, settore privato o singoli cittadini, devono riconoscere questa responsabilità condivisa, attivarsi per proteggersi e se necessario assicurare una risposta coordinata per rafforzare la cibersicurezza".

54. Ad opera del Regolamento (CE) 2004/460 del 10 marzo 2004.

55. Matassa 2023, p. 29.

56. L'imposizione agli Stati membri dell'Unione di adottare strategie nazionali era funzionale a garantire che i medesimi fossero in condizione di "reagire – attraverso il recupero dei servizi – a potenziali attacchi cibernetici distruttivi" (Borriello–Fristachi 2022, p. 162).

"operatori di servizi essenziali" e per i "fornitori di servizi digitali"[57].

Per entrambe le categorie di fornitori di servizi (pur con qualche differenza) la Direttiva prevedeva che gli Stati membri definissero obblighi di adozione di misure tecnico-organizzative (adeguate a gestire i rischi e a minimizzare l'impatto di incidenti[58]) e di notifica di incidenti aventi un impatto rilevante sulla continuità dell'erogazione dei servizi medesimi (anche nell'ottica di ricevere il supporto dell'Autorità nazionale competente e del CSIRT).

Nel 2017 è stata adottata la seconda *Strategia* in materia di cybersicurezza, imperniata sui tre concetti fondamentali di resilienza, deterrenza e difesa, che prefigurava la necessità della riforma dell'ENISA, riforma operata concretamente dal citato Regolamento (UE) 2019/881, che ha ridefinito poteri e funzioni dell'Agenzia (peraltro ridenominandola Agenzia dell'Unione europea per la cybersicurezza) e ha delineato un quadro comune europeo per la certificazione della sicurezza di prodotti e servizi ICT[59].

I poteri che il Regolamento attribuisce all'ENISA (di cui vengono sottolineate "l'indipendenza e la particolare 'capacità tecnica'") sono ampi, e volti, fondamentalmente, a fornire supporto alla Commissione e agli Stati membri "nell'elaborazione e nell'attuazione di politiche dell'Unione relative alla cybersicurezza, ivi comprese le politiche settoriali in materia di cybersicurezza" (art. 4, par. 2) e nello sviluppo delle capacità di prevenzione, rilevazione e analisi delle minacce informatiche e degli incidenti (art. 6), oltre che a rafforzare la cooperazione fra gli Stati e fra questi e l'Unione[60].

Del dicembre 2020 è invece la *EU's Cybersecurity Strategy for the Digital Decade*[61], avente quale elemento cardine "l'istituzione di un'unità congiunta per il ciberspazio (nota come Joint Cyber Unit o

57. Trattasi di categorie di fornitori di servizi considerati di particolare rilievo per il funzionamento delle società moderne (e del mercato interno). Gli operatori di servizi essenziali dovevano essere identificati (e inseriti in apposito elenco) dagli Stati membri sulla base di criteri definiti (invero in modo ampio e generico) dalla Direttiva e laddove tali operatori operino in un dei settori qualificato come essenziale dalla Direttiva medesima (all'Allegato II); i fornitori di servizi digitali venivano invece circoscritti a tre tipologie, identificate nell'Allegato III alla Direttiva, che richiamava i seguenti servizi: Mercato *online*; Motore di ricerca *online*; Servizi nella nuova (*cloud computing*).
58. La Direttiva non indicava direttamente la metodologia da utilizzare per la definizione delle misure di sicurezza, riconoscendo in questo senso ampia discrezionalità agli Stati. All'inevitabile rischio di frammentazione connesso a tale situazione ha fornito parziale di rimedio il gruppo di cooperazione dei CSIRT, che ha definito indicazioni e orientamenti (v. in particolare il *Reference document on security measures for Operators of Essential Services*, CG Publication 01/2018).
59. Tra gli obiettivi del Regolamento (secondo quanto previsto dall'art. 1, par. 1, del medesimo) vi era quello di definire "un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza dei prodotti TIC, servizi TIC e processi TIC nell'Unione, oltre che al fine di evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cibersicurezza nell'Unione". A tal fine il Regolamento dispone l'istituzione di un Quadro europeo di certificazione della cibersicurezza (il quale, secondo quanto previsto dall'art. 46, par. 2, "prevede un meccanismo volto a istituire sistemi europei di certificazione della cibersicurezza e ad attestare che i prodotti, servizi TIC e processi TIC valutati nel loro ambito sono conformi a determinati requisiti di sicurezza al fine di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti, servizi e processi o accessibili tramite essi per tutto il loro ciclo di vita") oltre che il varo, da parte della Commissione, di un "programma di lavoro progressivo dell'Unione per la certificazione europea della cibersicurezza" (art. 47).
60. L'attribuzione all'ENISA di compiti sostanzialmente consultivi è stata fatta oggetto di critiche, da parte della dottrina, che ha sottolineato come, a livello europeo, "sarebbe stato preferibile attribuire all'Agenzia funzioni maggiormente incisive, in considerazione della rilevanza del bene giuridico tutelato e della crescente esigenza di sicurezza informatica all'interno del mercato unico digitale" (così Previti 2022, p. 74).
61. Doc. JOIN(2020) 18.

JCU) come piattaforma virtuale e fisica per la cooperazione tra le varie comunità di cybersicurezza all'interno dell'Ue, ciò con particolare attenzione al coordinamento tecnico e operativo volto a contrastare gravi minacce e incidenti informatici di natura transfrontaliera"[62].

Con la Direttiva NIS II si è poi inteso innalzare ulteriormente il livello della cybersicurezza europea (anche alla luce delle emerse lacune della Direttiva NIS I), principalmente mediante ampliamento del novero dei fornitori di servizi (con il venir meno della distinzione tra fornitori di servizi essenziali e fornitori di servizi digitali) soggetti agli obblighi e agli adempimenti previsti dalla Direttiva stessa e, ciò che forse costituisce la novità più rilevante, tramite definizione di criteri più dettagliati per l'individuazione degli stessi, con correlativa diminuzione degli spazi di discrezionalità degli Stati membri. Inoltre, la Direttiva ha inteso procedere nel senso dell'implementazione di una politica di "coordinated vulnerability disclosure" prevedendo (all'art. 12) l'istituzione di una banca dati europea delle vulnerabilità e che i singoli Stati adottino proprie regolazioni concernenti le modalità di rilevamento delle vulnerabilità dei sistemi informatici[63].

Del 2024 è il *Cyber Resilience Act* (Regolamento (UE) 2024/2847), relativo ai requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali[64] mentre, da ultimo, occorre menzionare il *Cyber Solidarity Act* (Regolamento (UE) 2025/38), che contiene disposizioni atte a declinare il contrasto alla cybersicurezza in una logica sempre più "comunitaria", definendo un sistema "integrato" tra gli Stati membri atto a garantire la sicurezza informatica.

La prospettiva dalla quale il Regolamento ora citato prende le mosse è rappresentata dalla "necessità di rafforzare rilevamento e conoscenza situazionale delle minacce e degli incidenti informatici in tutta l'Unione e intensificare la solidarietà migliorando la preparazione e la capacità degli Stati membri e dell'Unione di prevenire gli incidenti di cybersicurezza significativi e gli incidenti di cybersicurezza su vasta scala e di rispondervi" (così il considerando n. 7).

In tale ottica, il Regolamento prevede l'istituzione di una rete paneuropea di Poli informatici (denominata *Sistema europeo di allerta per la cybersicurezza*) e di un "meccanismo per le emergenze di cybersicurezza", al fine in particolare di "sostenere gli Stati membri, su loro richiesta, nella preparazione e nella risposta agli incidenti di cybersicurezza significativi e agli incidenti di cybersicurezza su vasta scala, nell'attenuarne l'effetto e nell'avviare la ripresa dagli stessi" (così sempre il considerando n. 7).

La disamina dell'architettura e dell'insieme dei soggetti chiamati a realizzare gli obiettivi di cybersicurezza definiti dal Regolamento in parola offre spunti di sicuro interesse.

Il Regolamento, come accennato, prevede l'istituzione di un *Sistema europeo di allerta per la cybersicurezza* costituito da una "rete paneuropea di Poli informatici", la cui *mission* è costituita dallo sviluppo e dal potenziamento di "capacità coordinate in materia di rilevamento e capacità comuni in materia di conoscenza situazionale" (a fini di cybersecurity), e di cui fanno parte tanto Poli informatici nazionali quanto Poli informatici transfrontalieri.

I Poli informatici nazionali sono posti e agiscono "sotto l'autorità di uno Stato membro" (così come espressamente riconosciuto dall'art. 4, par. 2), e per quanto concerne la natura giuridica, la struttura e l'organizzazione dei medesimi il Regolamento lascia agli Stati ampia discrezionalità[65], ponendo requisiti invece più stringenti in riferimento a capacità funzionali e prestazionali[66].

62. Matassa 2023, p. 28 ss.

63. In tema Ricotta 2024, p. 82 ss.

64. Per approfondimenti si rimanda a Chiara 2023, p. 143 ss.

65. Ai sensi dell'art. 4, par. 2 del Regolamento, infatti, "può trattarsi di un CSIRT o, se del caso, di un'autorità nazionale di gestione delle crisi informatiche o di un'altra autorità competente designata o istituita a norma dell'articolo 8, paragrafo 1, della direttiva (UE) 2022/2555, o di un altro soggetto".

66. Più nello specifico, il Regolamento prevede che ciascun Polo informatico nazionale debba possedere la capacità "di fungere da punto di riferimento e da porta di accesso ad altre organizzazioni pubbliche e private a livello

Da un lato, dunque, il Regolamento riconosce ampia discrezionalità agli Stati membri per quanto concerne l'istituzione e la definizione delle caratteristiche dei Poli informatici nazionali, dall'altro, prevedendo i menzionati requisiti di capacità e prestazionali, pone "limiti esterni" a detta discrezionalità, richiedendo agli Stati membri di garantire l'idoneità dei propri Poli nazionali a rispettare gli standard e a conseguire gli obiettivi dallo stesso individuati.

Gli Stati possono poi scegliere di far aderire un proprio Polo informatico ad un Polo informatico transfrontaliero, organismo, quest'ultimo, definito come "una piattaforma multinazionale, istituita mediante un accordo di consorzio scritto, che riunisce in una struttura di rete coordinata i poli informatici nazionali di almeno tre Stati membri e che è concepita per migliorare il monitoraggio, il rilevamento e l'analisi delle minacce informatiche, per impedire gli incidenti informatici e per favorire l'elaborazione di analisi delle minacce informatiche, in particolare mediante lo scambio di dati e informazioni pertinenti, se del caso anonimizzati, nonché tramite la condivisione di strumenti all'avanguardia e lo sviluppo congiunto di capacità di rilevamento, analisi, prevenzione e protezione nel settore informatico in un contesto di fiducia" (art. 2, n. 1).

L'adesione di un Polo nazionale ad un Polo transfrontaliero (adesione che, lo si ribadisce, ha natura volontaria) implica l'impegno da parte del primo ad aderire ad un accordo di consorzio che prevede, fra le altre cose, lo scambio di rilevanti informazioni[67] e il perseguimento di determinati obiettivi di "sviluppo di strumenti e tecnologie avanzati, quali gli strumenti di intelligenza artificiale e di analisi dei dati" (art. 6, par. 2, lett. c)[68].

Oltre al descritto *Sistema europeo di allerta per la cybersicurezza*, il Regolamento prevede poi l'istituzione di un *Meccanismo per le emergenze informatiche* e di un *Meccanismo di riesame degli incidenti di cybersicurezza*.

Il primo persegue gli obiettivi di sostenere le azioni di preparazione di soggetti operanti in settori cruciali per la società, al fine di sondarne le capacità di resistenza nei confronti di eventuali minacce e creare una riserva dell'Ue per la cybersicurezza concernente servizi pronti per essere erogati su richiesta di Stati membri o istituzioni per aiutare i medesimi a gestire gli incidenti di cybersicurezza significativi o su vasta scala, ovvero garantire assistenza a uno Stato membro che stia a sua volta assistendo un altro Stato membro interessato da un incidente di cybersicurezza; il *Meccanismo di riesame degli incidenti di cybersicurezza* è invece volto a consentire agli organismi ed alle istituzioni dell'Unione e degli Stati membri di trarre insegnamenti dagli incidenti nell'ottica di migliorare le risposte agli incidenti medesimi.

Questi gli elementi più rilevanti del Regolamento (UE) 2025/38. L'analisi degli stessi, ma invero del complessivo quadro giuridico europeo in materia di cybersicurezza, consente di effettuare alcune considerazioni sul tema del rapporto tra *government* e *governance*, e di chiedersi se uno dei due (e nel caso quale) debba considerarsi prevalente rispetto all'altro, o comunque caratterizzante il sistema.

Nel rispondere positivamente, verrebbe quasi istintivo indicare, quale istituto caratterizzante la regolazione della cybersecurity, la *governance* (termine al quale, peraltro, molti degli atti esaminati fanno espresso richiamo), ma un'analisi più cauta

nazionale per la raccolta e l'analisi di informazioni sulle minacce e sugli incidenti informatici e per contribuire a un polo informatico transfrontaliero" (art. 4, par. 2, lett. a) ed essere in grado "di rilevare, aggregare e analizzare dati e informazioni relativi alle minacce e agli incidenti informatici, come le analisi sulle minacce informatiche, utilizzando in particolare tecnologie all'avanguardia, al fine di prevenire gli incidenti" (art. 4, par. 2, lett. b).

67. Tra le informazioni da porre ad oggetto di condivisione, secondo quanto disposto dall'art. 6, par. 1, quelle relative a "minacce informatiche, quasi incidenti, vulnerabilità, tecniche e procedure, indicatori di compromissione, tattiche avversarie, informazioni specifiche sugli autori delle minacce, allarmi di cybersicurezza e raccomandazioni relative alla configurazione degli strumenti di cybersicurezza per rilevare gli attacchi informatici, tra loro all'interno del polo informatico transfrontaliero".

68. In conclusione di questa assai sintetica disamina del Sistema europeo di allerta per la cybersicurezza delineato dal Regolamento (UE) 2025/38, si osserva poi che gli Stati che intendano aderire al medesimo sono tenuti a farsi carico di obblighi concernenti la garanzia di "un elevato livello di cybersicurezza" (secondo quanto previsto dall'art. 8) e il finanziamento del sistema e delle attività allo stesso riconducibili.

e meditata consente di delineare un quadro ben diverso, che restituisce una piena centralità al *government*, e dunque alla sovranità, degli Stati.

Ed infatti, in tutti gli atti (normativi e non) che compongono il quadro giuridico concernente la cybersicurezza europea viene affermato e ribadito, a riguardo di molti ambiti e profili, il rispetto, da parte dell'ordinamento unionale, della sovranità e della "discrezionalità politica" dei singoli Stati, cui è riconosciuta ampia autonomia nell'adozione delle misure ritenute necessarie a proteggere beni e valori essenziali – quali la sicurezza, l'ordine pubblico, il perseguimento di reati[69] – e nella definizione in concreto delle proprie Strategie nazionali, oltre che nella definizione dell'organizzazione amministrativa preposta a tale fine[70].

Rispetto, in particolare, all'ultimo profilo menzionato, si rileva che l'organismo europeo che occupa una posizione di centrale rilievo nell'ambito dell'architettura della cybersicurezza, l'ENISA, risulta essere titolare più di funzioni di supporto e cooperazione con le Autorità e gli organismi degli Stati membri che di prerogative e poteri suscettibili di vincolare unilateralmente (sul piano normativo o amministrativo) questi ultimi[71].

Per quanto concerne le Autorità nazionali competenti (la cui istituzione è stata prevista a partire dalla Direttiva NIS I), giova osservare che la normativa unionale lascia agli Stati grande libertà nel definirne natura e organizzazione: non a caso, nel panorama dei diversi ordinamenti degli Stati membri si rinvengono attribuzioni di funzioni di Autorità nazionali competenti tanto ad Autorità indipendenti quanto a enti governativi (Ministeri, Capi di Governo) o comunque in varia misura dipendenti dai governi[72].

69. In questo senso vanno, ad esempio, l'art. 1, par. 6, della Direttiva NIS I – il quale stabilisce che "la presente direttiva lascia impregiudicate le misure adottate dagli Stati membri per salvaguardare le funzioni essenziali dello Stato, in particolare di tutela della sicurezza nazionale, comprese le misure volte a tutelare le informazioni, la cui divulgazione sia dagli Stati membri considerata contraria agli interessi essenziali della loro sicurezza, e di mantenimento dell'ordine pubblico, in particolare a fini di indagine, accertamento e perseguimento di reati" (v. anche il considerando n. 8) – o i paragrafi 4 e 5 dell'art. 1 del Regolamento (UE) 2025/38 che prevedono, rispettivamente, che "le azioni intraprese a norma del presente regolamento sono realizzate nel debito rispetto delle competenze degli Stati membri e integrano le attività svolte dalla rete di CSIRT, da EU-CyCLONe e dal gruppo di cooperazione NIS" e che "il presente regolamento lascia impregiudicate le funzioni statali essenziali degli Stati membri, tra cui la garanzia dell'integrità territoriale dello Stato, il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza nazionale. In particolare, la sicurezza nazionale resta una competenza esclusiva di ciascuno Stato membro".

70. Trattasi invero di approccio che appare (ed è forse l'unico possibile, in questo senso) conforme all'art. 4, par. 2, del Trattato sull'Unione europea, il quale stabilisce che l'Unione "rispetta le funzioni essenziali dello Stato, in particolare le funzioni di salvaguardia dell'integrità territoriale, di mantenimento dell'ordine pubblico e di tutela della sicurezza nazionale. In particolare, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro".

71. Ed infatti, "l'attività principale dell'ENISA è quella di coordinare l'operato degli stati membri e favorire il dialogo intra-europeo, attraverso l'elaborazione di linee guida e l'individuazione di best practices. A questo scopo, l'agenzia pubblica molti documenti, disponibili online e liberamente consultabili, per cercare di tenere aggiornato lo stato dell'arte della cybersecurity in Europa e stimolare il confronto tra i vari stati, nell'intento che si affermino le pratiche più avanzate" (così Cencetti 2014, p. 26). In questo senso v. anche Bruno 2020, p. 13 s., che sottolinea come spia dell'approccio "rispettoso delle prerogative degli Stati membri in materia di disciplina delle attività di sicurezza sia rappresentata anche dalla configurazione dell'ENISA quale 'organo tecnico di assistenza alla Commissione europea ed agli Stati membri'".

72. Sono scelte riconducibili a quel fenomeno che è stato descritto in termini di "verticalizzazione della leadership in campo cyber a favore dei capi di governo, incentivata dalla necessità di evitare la frammentazione del potere in questi ambiti" (cfr. Longo 2024-a, p. 328). Si tratta di un processo che è stato commentato anche criticamente da quella parte di dottrina che vede con preoccupazione il protagonismo degli apparati governativi e spazi limitati per il controllo parlamentare e la partecipazione dei cittadini (su queste posizioni, tra gli altri, Pietrangelo 2024, p. 14 s. e Moroni 2024, *passim*).

Le scelte dell'ultimo tipo mostrano la volontà degli Stati di prevedere l'inserimento delle Autorità di cybersicurezza nel circuito governativo, e di fare delle stesse (anche) strumento di definizione e attuazione di politiche, facendo risultare l'aspetto politico-decisionale predominante su quello tecnico (che sarebbe invece risultato prevalente a fronte della individuazione di Autorità amministrative indipendenti).

Dunque, se da un lato l'istituzione di un apposito ente (e più in generale di un apparato amministrativo), attività che rientra nel novero dei metodi di risposta degli Stati "alle tradizionali minacce sperimentate nell'arena materiale di espressione della [propria] sovranità"[73], ha in questo caso una provenienza esogena rispetto ai meccanismi politico-decisionali degli Stati, l'esatta collocazione di tale ente (apparato) nel quadro costituzionale e dell'organizzazione amministrativa dello specifico ordinamento considerato risulta essere di esclusivo appannaggio degli Stati.

A fronte delle riportate considerazioni, mi pare che da un'analisi dell'evoluzione che il quadro normativo europeo in materia di cybersicurezza ha conosciuto negli anni emerga chiaramente come quelli che pure possono essere qualificati quali modelli di *governance* – nelle loro varie possibili declinazioni – mostrino la piena centralità del *government* per quanto concerne la regolazione del cyberspazio.

Ed infatti, se appare lecito parlare eventualmente di quella che è stata definita "sleeping sovereignity, che si desta solo quando essa stessa valuta opportuno destarsi"[74], e/o di un (volontario e deliberato) arretramento della decisione politica in favore di una regolazione avente un indubitabile contenuto tecnico (e il cui sviluppo richiede un necessario – ma comunque voluto, dalla parte pubblica-statuale – coinvolgimento di attori privati) resta il fatto che la costruzione dell'architettura della cybersicurezza unionale non prescinde affatto dal *government* dei singoli Stati e, anzi, ne conferma la piena presenza, quale espressione di quella "sovranità digitale" che si concretizza nella capacità di questi ultimi (e di riflesso della stessa Unione europea) "to act independently in the digital world", anche in riferimento alle questioni concernenti la regolazione e la gestione del cyberspazio[75].

L'affermazione della effettività della sovranità digitale impone di tener conto delle caratteristiche del cyberspazio e del tema della interconnessione/interdipendenza in materia di cybersicurezza – e quindi di strutturare un'architettura normativo-organizzativa che preveda anche forme di cooperazione con Enti e organismi di altri ordinamenti e di scambio di buone pratiche e informazioni – senza che ciò si traduca nello slittamento del *government* in forme di *governance* (le quali, come detto, prevedono processi decisionali aventi carattere prevalentemente orizzontale e condiviso, e in cui le decisioni politiche dei singoli Stati assumono carattere recessivo, venendo condizionate al punto da perdere il proprio contenuto e le proprie caratteristiche connotative).

Ulteriori conferme a tale conclusione provengono da alcune scelte normativo-regolatorie effettuate dall'ordinamento italiano, nell'ambito del quale si è venuto a definire un quadro giuridico del quale possono individuarsi alcuni elementi caratterizzanti.

Un primo elemento è costituito dalla centralità del ruolo assunto dal Presidente del Consiglio dei Ministri, centralità che si rinviene fin dalle prime disposizioni riferibili al tema (ed in specie quelle concernenti il "Sistema di informazione per la sicurezza della Repubblica", disegnato dalla legge 3 agosto 2007, n. 124[76]) e che risulta successivamente confermata da quelle attuative degli atti normativi

73. Così Giupponi 2024, p. 277.

74. Così Chessa 2019, p. 328.

75. La citazione è tratta dal documento dell'European Parliamentary Research Service *Digital sovereignty for Europe* del luglio 2020 (p. 1). Osservano in tema Sorrentino–Spagnuolo 2024, p. 689, che il concetto di sovranità digitale indica "la capacità di un Paese di esercitare autorità all'interno del cyberspazio, garantendo l'indipendenza tecnologica e il controllo sui dati personali". Sul concetto di sovranità digitale e sulle questioni regolatorie concernenti il web v. anche Bertola 2022, p. 39 ss. e Santaniello 2022, p. 47 ss.

76. Ai sensi della legge in parola, al Presidente del Consiglio dei Ministri spetta tra le altre cose "l'alta direzione e la responsabilità generale della politica dell'informazione per la sicurezza, nell'interesse e per la difesa della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento" (così l'art. 1, comma 1,

europei (o che con questi ultimi erano comunque tenute a fare i conti).

Senza ripercorrere l'articolata evoluzione del quadro normativo, e soffermandoci esclusivamente sulle disposizioni vigenti, si rileva che il d.l. n. 82/2021 assegna al Presidente del Consiglio un complesso di compiti e funzioni che fanno del medesimo la figura cardine nella definizione delle politiche di cybersicurezza e delle misure di direttiva e indirizzo ai fini dell'attuazione delle stesse.

Ai sensi dell'art. 2, comma 1, del decreto-legge in parola, spettano in particolare al Presidente del Consiglio dei Ministri "a) l'alta direzione e la responsabilità generale delle politiche di cybersicurezza; b) l'adozione della strategia nazionale di cybersicurezza, sentito il Comitato interministeriale per la cybersicurezza (CIC) […]; c) la nomina e la revoca del direttore generale e del vice direttore generale dell'Agenzia per la cybersicurezza nazionale […] previa deliberazione del Consiglio dei ministri".

Numerose e rilevanti funzioni sono poi attribuite al Presidente del Consiglio dei Ministri dal c.d. Decreto *perimetro* (d.l. 21 settembre 2019, n. 105, recante *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*), specie a riguardo dell'individuazione dei soggetti e degli enti da includersi nel "perimetro di sicurezza nazionale cibernetica", in quanto tali tenuti al rispetto delle misure e degli obblighi previsti dal medesimo decreto, nonché dagli atti di recepimento delle Direttive europee NIS I e NIS II

lett. a), il coordinamento delle politiche dell'informazione per la sicurezza (e l'adozione, a tale fine, di apposite direttive sentito il Comitato interministeriale per la sicurezza della Repubblica) e un potere di carattere residuale funzionale all'emanazione di "ogni disposizione necessaria per l'organizzazione e il funzionamento del Sistema di informazione per la sicurezza della Repubblica" (per tutte le funzioni da ultime citata v. l'art. 1, comma 3, della legge in esame). Ai sensi del comma 3-*bis* dell'art. 1 della l. n. 124 del 2007 (inserito dall'articolo 1, comma 1, della l. 7 agosto 2012, n. 133) "il Presidente del Consiglio dei Ministri, sentito il Comitato interministeriale per la sicurezza della Repubblica, impartisce al Dipartimento delle informazioni per la sicurezza e ai servizi di informazione per la sicurezza direttive per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali". Per quanto concerne il tema del raccordo tra l'azione del Presidente del Consiglio e il Parlamento, l'art. 38, comma 1-*bis*, della legge n. 124 prevede che il Governo alleghi alla relazione sulla politica dell'informazione per la sicurezza e sui risultati ottenuti, che è tenuto a presentare annualmente al Parlamento, "un documento di sicurezza nazionale, concernente le attività relative alla protezione delle infrastrutture critiche materiali e immateriali, nonché' alla protezione cibernetica e alla sicurezza informatica". In attuazione del citato comma 3-*bis*, con d.P.C.M. 19 marzo 2013, n. 66, è stata adottata un'apposita Direttiva "recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale", avente il fine specifico di definire, a legislazione vigente, un quadro strategico nazionale, "con la specificazione dei ruoli che le diverse componenti istituzionali devono esercitare per assicurare la sicurezza cibernetica del Paese e la predisposizione di meccanismi e procedure di azione secondo un approccio interdisciplinare e coordinato, su più livelli, che coinvolga tutti gli attori pubblici, ferme restando le attribuzioni previste dalla normativa vigente per ciascuno di essi, nonché gli operatori privati interessati" (così il Preambolo). La Direttiva, in tale ottica, delineava un'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, articolata su tre distinti livelli d'intervento, di cui il primo di indirizzo politico e coordinamento strategico (teso all'individuazione degli obiettivi anche attraverso l'elaborazione di un Piano nazionale per la sicurezza dello spazio cibernetico), il secondo "di supporto" e di attuazione di quanto definito al primo livello (in particolare nell'ambito della pianificazione), il terzo di gestione delle crisi, con il compito di curare e coordinare le attività di risposta e di ripristino della funzionalità dei sistemi, avvalendosi di tutte le componenti interessate. Alla Direttiva del 2013 ha fatto poi seguito quella del 2015, in precedenza citata. L'architettura originariamente disegnata dal d.P.C.M. del 2013 è stata poi successivamente modificata ad opera del d.P.C.M. 17 febbraio 2017, n. 85, che ha ampliato le funzioni del Presidente del Consiglio dei Ministri, introdotto le definizioni di operatori di servizi essenziali e di fornitori di servizi digitali e previsto, in un apposito articolo (il 6) specifiche linee di azione per la sicurezza cibernetica.

(rispettivamente d.l. 18 maggio 2018, n. 65 e 4 settembre 2024, n. 138, con quest'ultimo che ha abrogato il primo).

Come è stato osservato, dal complesso dei menzionati atti normativi emerge con chiarezza una "notevole scelta accentratrice in materia di cybersicurezza", tesa "ad evitare che tendenze centrifughe – sia interne allo Stato sia esterne ad esso – possano compromettere lo svolgimento di quelle funzioni essenziali della Nazione che si realizzano mediante l'uso di reti e sistemi informatici"[77].

Il carattere "accentrato" (e "incentrato" sul Governo e sul Presidente del Consiglio) dell'architettura della cybersecurity nazionale è confermato dalle scelte concernenti la struttura e la natura delle Autorità e dei diversi organismi previsti dalle disposizioni europee e facenti parte (a vario titolo) dell'architettura della cybersicurezza.

Per quanto concerne "l'Autorità nazionale competente", il nostro Legislatore non ha optato per il modello dell'Autorità indipendente, bensì per quello dell'Agenzia, della quale peraltro il Presidente del Consiglio (o l'Autorità delegata eventualmente istituita) si avvale (secondo quanto espressamente stabilito dall'art. 5, comma 2, del d.l. n. 82/2021)[78].

L'Agenzia per la cybersicurezza nazionale, posta "sotto la guida politica del Presidente del Consiglio dei Ministri"[79], svolge peraltro anche funzioni di Punto di contatto unico NIS, di Gruppo nazionale di risposta agli incidenti di sicurezza informatica (il CSIRT, ovvero l'organo preposto alle funzioni di gestione degli incidenti di sicurezza informativa per i settori, i sottosettori e le tipologie di soggetti individuati e definiti dal d.lgs n. 138/2024, e in specie dall'art. 15 del medesimo), di Autorità nazionale di gestione delle crisi informatiche, di Autorità nazionale di certificazione della cybersicurezza – ai sensi dell'articolo 58 del regolamento (UE) 2019/881 – e di Autorità competente per l'esecuzione dei compiti previsti dal regolamento delegato (UE) 2024/1366 della Commissione.

Si tratta, in larga misura, di funzioni di natura tecnica, che l'Agenzia è chiamata a svolgere anche in cooperazione con le altre Autorità nazionali e gli altri organismi previsti a livello europeo, nonché di funzioni di supporto all'autorità governativa, e in specie al Presidente del Consiglio dei Ministri, cui, a riguardo di molti profili, spetta l'assunzione delle decisioni "finali", che hanno ovviamente natura politico-amministrativa (natura che prevale su quella tecnica, pur presente[80]).

77. Longo 2024-a, p. 337.

78. L'Agenzia gode di alcune forme di autonomia, ad essa specificamente riconosciute dalla legge. In particolare, ai sensi dell'art. 5, comma 2, del d.l. n. 82 del 2021, la medesima "è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria", ancorché nei limiti previsti dal medesimo decreto; ciò farebbe dell'ACN un'Agenzia caratterizzata da "una più marcata autonomia rispetto ad altre agenzie", tale da collocarla "al di fuori del modello di agenzia creato dal d.lgs. n. 300/1999" (cfr. il dossier del Servizio Studi di Camera e Senato - A.C. 3161, Dossier su "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*", 23 luglio 2021, p. 19 ss.). La sussistenza dei descritti ambiti di autonomia non è in ogni caso sufficiente a colmare lo spazio che separata il modello delle Agenzie da quello delle Autorità indipendenti (in questo senso cfr. Calzolaio 2024, p. 102), e a ricondurre dunque l'ACN a questo secondo novero.

79. Forgione 2022, p. 1120.

80. Ai sensi dell'art. 7 del d.l. n. 82 del 2021, l'Agenzia, tra le altre cose, predispone (lett. b) la Strategia nazionale di cybersicurezza, che viene poi adottata dal Presidente del Consiglio, sentito il Comitato interministeriale per la cybersicurezza, e svolge (lett. c) "ogni necessaria attività di supporto al funzionamento del Nucleo per la cybersicurezza" – il quale, a sua volta, ai sensi dell'art. 8, comma 1, del medesimo decreto, svolge funzioni di "supporto del Presidente del Consiglio dei ministri nella materia della cybersicurezza, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento" – oltre a supportare "il Presidente del Consiglio dei ministri ai fini dell'articolo 1, comma 19-*bis*, del decreto-legge perimetro" (lett. i). A ciò aggiungasi che, secondo quanto stabilito dall'art. 6 della l. 28 giugno 2024, n. 90, il Presidente del Consiglio dei Ministri, sentiti il direttore generale del Dipartimento delle informazioni per la sicurezza e il direttore generale dell'Agenzia per la cybersicurezza nazionale, "può disporre il differimento degli obblighi informativi cui è in ogni caso tenuta l'Agenzia ai sensi delle disposizioni vigenti, ivi compresi quelli

4. Osservazioni conclusive

Alla luce di quanto si è illustrato nel corso del presente contributo, mi pare che possa affermarsi con relativa sicurezza che la *race for the cyberspace* vede un chiaro protagonismo degli Stati (e quindi degli ordinamenti statuali), i quali da un po' di tempo a questa parte sembrano aver pienamente compreso l'importanza del cyberspazio e la rilevanza delle minacce e degli incidenti informatici, che possono essere utilizzati anche per finalità geopolitiche (e di *cyberwarfare*).

Minacce e incidenti possono produrre conseguenze di estremo rilievo, pregiudicando l'erogazione di servizi, alterando il funzionamento dei mercati, sottraendo dati rilevanti (e sensibili) per utilizzi anche illeciti e in vari modi incidendo su diritti e libertà fondamentali dei cittadini.

Si tratta, dunque, come in precedenza si accennava, di difendere e salvaguardare valori e beni garantiti dalle Carte costituzionali di gran parte degli ordinamenti giuridici contemporanei: in particolare, oltre ai singoli diritti e alle singole libertà, vengono in rilievo la sicurezza pubblica, la difesa, e invero lo stesso corretto funzionamento dei sistemi democratici (dato che le minacce e gli incidenti informatici possono interferire con le funzioni degli organi costituzionali e a rilevanza costituzionale).

Di qui la sempre più sentita esigenza di costruire architetture organizzative e politiche di cybersicurezza volte a scongiurare minacce o incidenti e/o a minimizzarne l'impatto (ove l'attività di prevenzione risulti inefficace) e, parallelamente, a sviluppare la cyber-resilienza di sistemi e reti informatiche.

La definizione, tuttavia, di architetture di sistemi di cybersicurezza nazionali può produrre riflessi sul funzionamento complessivo del cyberspazio (luogo che, lo si è detto, è oggi insostituibile per lo svolgimento di gran parte delle attività che caratterizzano la quotidianità degli individui e il funzionamento dei mercati), i cui "luoghi" e le cui "componenti" sono, come illustrato, interconnessi a livello globale.

La regolamentazione di un oggetto avente simili caratteristiche, e l'esigenza degli Stati di non spogliarsi di proprie prerogative sovrane (evenienza inaccettabile stante il valore degli interessi in gioco), sembra imporre la definizione di regole condivise, secondo i classici moduli e schemi del diritto internazionale[81].

Non si è tuttavia ancora addivenuti alla definizione di simili regole (essendoci fino ad ora limitati alla sottoscrizione di documenti – come il *Cyber Defence Pledge* firmato al vertice NATO di Varsavia del 2016 – contenenti impegni aventi un'efficacia vincolante relativa) e forse tale obiettivo non verrà mai conseguito: e ciò anche in ragione del fatto che se il cyberspazio ha, come detto, caratteristiche di "luogo", lo stesso non è un territorio (essendo, anzi, connotato da de-territorialità), di talché rispetto ad esso non si tratta tanto di definire regole concernenti il regime giuridico di aree (e la misura della sovranità che i singoli Stati hanno su di essi) quanto piuttosto di regolamentare il funzionamento di attività e servizi e stabilire norme e obblighi atti ad assicurare che lo scambio di dati e informazioni sulle reti avvenga con determinate garanzie di non accadimento di incidenti informatici.

previsti ai sensi dell'articolo 17, commi 4 e 4-*bis*, del decreto-legge n. 82 del 2021, nonché il differimento di una o più delle attività di resilienza di cui all'articolo 7, comma 1, lettere n) e n-*bis*), del medesimo decreto-legge" a fronte di informativa ricevuta dalle Agenzie di informazione e sicurezza esterna e interna (disciplinate rispettivamente dagli articoli 6 e 7 della l. 3 agosto 2007, n. 124) che indichi il differimento come strettamente necessario "per il perseguimento delle finalità istituzionali del Sistema di informazione per la sicurezza della Repubblica". Anche in questo caso, esigenze concernenti la tutela di interessi fondamentali dello Stato, la cui valutazione è affidata al Presidente del Consiglio dei Ministri, sono destinate a prevalere su quelle concernenti l'adempimento, da parte dell'Agenzia nazionale per la cybersicurezza, degli obblighi sulla stessa incombenti.

81. Il parallelismo con la regolamentazione degli spazi marini appare in questo senso calzante. Osserva sul punto Calabrese 2025 che "come le acque internazionali, il cyberspazio è un dominio condiviso, dove diverse entità, siano esse statali o private, operano in uno spazio senza confini fisici definiti. Tuttavia, mentre le acque internazionali sono regolate da convenzioni globali come la Convenzione delle Nazioni Unite sul Diritto del Mare (UNCLOS), il cyberspazio non dispone ancora di un quadro normativo altrettanto consolidato. Ciò crea un vuoto regolamentare che complica la governance e l'attribuzione delle responsabilità".

Il quadro è reso però complicato dal fatto che i singoli Stati non sempre sono disposti a condividere le informazioni che riguardano la cybersicurezza (con il termine informazione intendiamo qui riferirci tanto ai dati – e agli elementi "di fatto" che risultano rilevanti rispetto ad una determinata fattispecie e a una possibile minaccia – quanto alle conoscenze tecniche necessarie per costruire un sistema di difesa dagli attacchi che risulti efficace ed efficiente), considerato quanto le stesse possono risultare sensibili e rilevanti per la protezione di beni giuridici di rango anche costituzionale; ciò pone un freno allo *sharing* (delle informazioni), il che, a sua volta, limita l'efficacia delle azioni concernenti la cybersicurezza.

In tema, sarà importante osservare l'impatto che avrà il Regolamento (UE) 2025/38, il quale rileva che lo scambio di informazioni costituisce una delle attività che si pongono alla base del funzionamento dei Poli informatici transfrontalieri e che risulta funzionale a consentire ai Poli stessi, e a quelli nazionali, di "migliorare il monitoraggio, il rilevamento e l'analisi delle minacce informatiche", a "impedire gli incidenti informatici" e di "favorire l'elaborazione di analisi delle minacce informatiche" (così l'art. 2, n. 1, recante la definizione di "Polo informatico transfrontaliero", e l'art. 5, par. 4)[82].

Non a caso, il Regolamento contiene specifiche disposizioni atte a favorire – nell'ottica della costituzione del *Sistema europeo di allerta per la cybersicurezza* – la cooperazione e lo scambio di informazioni tra Poli informatici transfrontalieri e Poli informatici nazionali facenti parte di Poli informatici transfrontalieri (così in particolare l'art. 6), oltre che tra Poli informatici transfrontalieri e la rete di CSIRT (così l'art. 7), prevedendo altresì che la scelta degli Stati membri di far aderire a un Polo informatico transfrontaliero un proprio Polo informatico imponga a quest'ultimo di aderire ad un accordo di consorzio che preveda, tra le altre cose, di "mettere in comune i dati e le informazioni pertinenti sulle minacce e sugli incidenti informatici provenienti da varie fonti all'interno dei poli informatici transfrontalieri e condividere informazioni analizzate o aggregate attraverso i poli informatici transfrontalieri, se del caso con la rete di CSIRT" (art. 3, par. 2, lett. b).

Alla base dell'adesione ai Poli informatici transfrontalieri vi è, però, come si precisava in precedenza, una scelta volontaria degli Stati, ai quali peraltro il Regolamento riconosce la possibilità di escludere la comunicazione di informazioni "la cui divulgazione sarebbe contraria agli interessi essenziali degli Stati membri in materia di sicurezza nazionale, pubblica sicurezza o difesa" (art. 1, par. 6); ne discende, a riguardo del profilo dello *sharing* delle informazioni, la constatazione che la scelta della definizione delle modalità di "presenza" nel cyberspazio e di contrasto e reazione a minacce e incidenti informatici resti saldamente in capo ai singoli Stati, che possono decidere – con decisione di natura politico-amministrativa – di aprirsi o meno alla cooperazione effettuando un bilanciamento tra la scelta di migliorare l'efficacia e l'efficienza della propria cybersicurezza (cooperando con organismi e Autorità di altri Stati e dell'Ue) e quella di mantenere la segretezza su determinati dati e informazioni.

Anche poi rispetto alla definizione dell'architettura istituzionale-amministrativa della *cybersecurity* si rinvengono elementi che confermano la piena presenza del *government* statale.

Considerato che, come è stato condivisibilmente affermato, l'organizzazione amministrativa (che ha una natura "funzionalizzata" in quanto si definisce in ragione degli obiettivi e delle funzioni da svolgersi per conseguirli[83]) costituisce "il più efficace e potente meccanismo di comando di cui disponga l'autorità, la più vasta e potente articolazione di dominio presente nell'ordinamento"[84], la medesima ha strettamente "a che fare" con la sovranità, la quale si declina, in questo senso, nella possibilità, per gli Stati, di definire la propria

82. Allo scambio di informazioni l'ordinamento unionale ha fin dalle origini riconosciuto un ruolo primario, nella definizione delle politiche (e degli obblighi) in materia di cybersicurezza. La Direttiva NIS I, ad esempio, qualificava detta attività come uno dei principali fattori di rafforzamento della cooperazione strategica fra gli Stati (e proprio con obiettivi di *information sharing* fu istituito il gruppo di cooperazione tra i CSIRT).

83. In questo senso cfr. Allegretti 2000, pp. 403 s., il quale osserva che "l'organizzazione non può non adeguarsi alle necessità della funzione" e che "è la funzione che determina il modo d'essere dell'organo".

84. Perfetti 2019, p. 65.

organizzazione (amministrativa) in modo pieno e in assenza di interferenze "esterne"[85].

Se le cose stanno in questi termini, deve allora concludersi che laddove tale organizzazione, o anche solo una parte di essa, risulti definita secondo modalità non riconducibili alla volontà politica di uno Stato (come concretizzatasi alla luce dei processi e degli schemi individuati dal quadro costituzionale di riferimento), la sovranità di quest'ultimo ne risulta affievolita.

Tale affievolimento può poi risultare da una scelta dello Stato, ovvero da un'imposizione di provenienza esterna allo stesso (e dal medesimo non voluta): solo in tale seconda ipotesi può in ipotesi parlarsi di effettivo "affievolimento", dato che nel primo caso pare più corretto ragionare di limitazione o "cessione" di sovranità (o al più di *sleeping sovereignty*), e dunque, di fatto, di *esercizio* di sovranità (secondo una specifica modalità, quella della auto-limitazione da parte dello Stato).

Ciò detto, giova richiamare che, rispetto al tema in esame, si rinviene un quadro di norme dell'Unione europea che è andato articolandosi e stratificandosi nel tempo, anche in riferimento ai profili della *governance* e dell'organizzazione amministrativa delle funzioni concernenti la cybersicurezza.

A partire in particolare dalla Direttiva NIS I, si è prevista l'istituzione di enti e organismi ascrivibili all'organizzazione amministrativa dei singoli Stati membri, ed in particolare Autorità nazionali competenti, Punti di contatto unici, Gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) e altri ancora.

A differenza di come ha operato in altri settori (si pensi a quelli dell'energia e del gas), nei quali all'obbligo, per gli Stati membri, di istituzione di enti o autorità pubbliche l'Unione europea ha fatto corrispondere la necessità della previsione, nell'ambito delle rispettive discipline istitutive, di contenuti minimi (atti ad esempio a garantire l'indipendenza e la funzionalità delle autorità), rispetto agli enti e agli organismi concernenti l'ambito della cybersicurezza l'ordinamento europeo riconosce agli Stati una ampia discrezionalità nella definizione della natura, dell'organizzazione e delle modalità di funzionamento degli stessi, non richiedendo la sussistenza della caratteristica dell'indipendenza degli organismi ma imponendo requisiti prestazionali e di idoneità a conseguire gli obiettivi: rispetto a tale quadro appare pienamente condivisibile l'osservazione secondo la quale, rispetto al quadro giuridico in materia di cybersecurity che si rinviene a livello sia europeo che nazionale, "l'autorità può non essere dotata del requisito dell'indipendenza, ma non può perdere quello della specializzazione, spesso della iper-specializzazione, tecnica"[86].

Altri esempi potrebbero poi essere riportati, ma il quadro pare ormai (almeno a chi scrive) sufficiente chiaro.

Dal medesimo, come si è più volte detto e argomentato nel corso del presente contributo, a riguardo del cyberspazio e delle funzioni di cybersicurezza emerge una compenetrazione tra modelli di *governance* e di *government*, con la prima che, lungi dal costituire un fattore di arretramento o "dissolvimento" delle sovranità statuali, pare configurare piuttosto una modalità specifica di esercizio di quest'ultima rispetto ad un oggetto, il cyberspazio, avente caratteristiche particolarissime (la sua natura mista fisico-virtuale, l'alto grado di interconnessione e interdipendenza fra le sue componenti, la sua rilevanza per l'esercizio di diritti e libertà fondamentali degli individui, gli effetti potenzialmente devastanti degli incidenti informatici…).

Nel cyberspazio gli Stati hanno compreso di poter (ambire a) esprimere la propria volontà di potenza, ma al contempo vedono nel medesimo

85. Richiamando le precedenti osservazioni concernenti l'individuazione del novero delle potestà pubbliche che possono ritenersi rientrare nelle prerogative della sovranità, si osserva che l'organizzazione costituisce uno degli elementi costitutivi degli ordinamenti giuridici, si può affermare, con relativa sicurezza, che la potestà di un ordinamento (*rectius*: dei poteri a ciò abilitati dal quadro normativo e costituzionale) di definire liberamente l'organizzazione degli uffici e degli organi titolari di potestà normative e amministrative costituisca una delle potestà direttamente connesse alla sovranità. In altre parole, se è vero (come è vero) che la sovranità implica che lo Stato è "libero di prendere, all'interno delle sue frontiere, tutte le decisioni amministrative e politiche che più gli convengono, fuori da ogni ingerenza da parte di uno Stato straniero" (così Freund 2008, p. 105), nel novero di tali decisioni rientrano indubbiamente quelle concernenti le predette istanze organizzative.

86. Calzolaio 2024, p. 105.

un fronte sterminato e difficilmente controllabile di potenziali attacchi, anche portati da altri Stati sovrani: tali constatazioni non offrono particolari margini allo sviluppo di schemi di *governance* alternativi al *government*, e ritengo non li offriranno mai.

Per tali ragioni, gli Stati tengono "stretta a sé" la cybersicurezza, allocando (non a caso) spesso e volentieri le funzioni alla medesima connesse al livello governativo.

Nel descritto quadro, ogni apertura a modelli di *governance* risponde sempre, in ultima istanza, a obiettivi e interessi dei singoli Stati, che possono rendere *dormiente* la propria sovranità e accettare forme di cooperazione, scambi di informazione o imposizione di regole se ciò consente a tali interessi (abbiano, gli stessi, natura economico-commerciale, (geo)politica, militare, sociale…) di meglio prosperare.

Non a caso, la mancata definizione di regole condivise a livello globale concernenti specificamente il cyberspazio non ha impedito a molti soggetti (compresi organizzazioni internazionali e Stati) di affermare come al cyberspazio medesimo si applichino le norme del diritto internazionale, comprese quelle relative al riconoscimento e al rispetto della sovranità sia interna che esterna degli Stati[87].

Un'applicazione (che invece altri contestano) che in ogni caso non potrà prescindere da qualche "adattamento": lo impone la natura del cyberspazio, il suo essere un luogo-non luogo, che richiede di pensare all'occupazione del territorio non in termini di invasione di aree territoriali (se si esclude il caso estremo dell'occupazione o della distruzione fisica di infrastrutture) bensì quale attività concernente l'acquisizione, senza il consenso dei legittimi titolari, di codici, protocolli e dati, oltre che la capacità di aggirare le difese informatiche di Stati, organizzazioni, imprese e individui.

È a tutto ciò che la definizione di modelli di *governance* è strumentale, non a consentire lo sviluppo di attività, mercati e/o processi decisionali a prescindere (o a scapito) dagli Stati; possiamo allora concludere affermando che il Leviatano è vivo e vegeto – come peraltro indirettamente conferma il *ReArm Europe Plan*, che è piano di riarmo degli Stati, non dell'Ue, e nel quale peraltro il tema della cybersicurezza non trova spazi – e "tenacemente presente" anche nelle datificate contrade della rete, e più in generale in quel "mondo nuovo che molti attendevano all'apparire della globalizzazione e della integrazione economica"[88].

Riferimenti bibliografici

U. Allegretti (2000), *La verità è nell'assunto: Stato e Istituzioni nel pensiero di Feliciano Benvenuti*, in "Jus", 2000, n. 3

A.C. Amato Mangiameli (2000), *Diritto e Cyberspace. Appunti di informatica giuridica e filosofia del diritto*, Giappichelli, 2000

A. Barletta (2019), voce *Governance [dir. Cost.]*, in "Enciclopedia Treccani online", 2019

V. Bertola (2022), *La sovranità digitale e il futuro di Internet*, in "Rivista italiana di informatica e diritto", 2022, n. 1

J. Bodin (1576/1964), *Les six livres de la republique*, Paris, 1576 [trad. it. a cura di M. Isnardi Parente], UTET, I, 1964

G. Borriello, G. Fristachi (2022), *Stato (d'assedio) digitale e strategia italiana di cybersicurezza*, in "Rivista di Digital Politics", 2022, n. 1-2

B. Bruno (2020), *Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali*, in "federalismi.it", 2020, n. 14

87. Per un inquadramento del tema cfr. Zorzi Giustiniani 2021 e Ruotolo 2021, p. 701 ss.

88. Cfr., per entrambe le citazioni, Cassese 2016, p. 45, che sul punto peraltro cita King–Lieberman 2009, p. 550.

D.L. Calabrese (2025), *Chi controlla il cyberspazio? La zona grigia della responsabilità*, in "AgendaDigitale", 12 febbraio 2025

S. Calzolaio (2024), *Autorità indipendenti e di governo della società digitale*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi et al., "La regolazione europea della società digitale", Giappichelli, 2024

S. Calzolaio (2023), *Vulnerabilità della società digitale e ordinamento costituzionale dei dati*, in "Rivista italiana di informatica e diritto", 2023, n. 2

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

S. Cassese (2025), *L'Europa si difenda*, in "Corriere della Sera", 13 marzo 2025

S. Cassese (2016), *Territori e potere. Un nuovo ruolo per gli Stati*, il Mulino, 2016

C. Cencetti (2014), *Cybersecurity: Unione europea e Italia. Prospettive a confronto*, Edizioni Nuova Cultura, 2014

O. Chessa (2025), *Realismo geopolitico e volontà statale*, in "Diritto Costituzionale", 2025, n. 1

O. Chessa (2019), *Dentro il Leviatano. Stato, sovranità e rappresentanza*, Mimesis Edizioni, 2019

O. Chessa (2002), *Libertà fondamentali e teoria costituzionale*, Giuffrè, 2002

P.G. Chiara (2023), *Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali*, in "Rivista italiana di informatica e diritto", 2023, n. 1

C. Colapietro (2023), *Gli algoritmi tra trasparenza e protezione dei dati personali*, in "federalismi.it", 2023, n. 5

C. Colapietro (2021), *Circolazione dei dati, automatizzazione e regolazione*, in "Osservatorio sulle fonti", 2021, n. 2

A. Contaldo, L. Salandri (2020), *La disciplina della cybersicurezza nell'Unione Europea*, in A. Contaldo, D. Mula (a cura di), "Cybersecurity Law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche", Pacini Giuridica, 2020

D. Djurdjevic, M. Stevanovic (2016), *The Value Challenge of Interconnectedness in Cyberspace for National Security*, Sinteza, 2016

N. De Felice, (2012), *Strategia di difesa nel cyberspazio quale contributo alla tutela degli interessi nazionali*, in U. Gori, L.S. Germani (a cura di), "Information Warfare 2011. La sfida della Cyber Intelligence al sistema Italia dalla sicurezza delle imprese alla sicurezza nazionale", Franco Angeli, 2012

M. D'Orsogna (2024), *Povertà sanitaria e welfare generativo: nuovi orizzonti e nuove sfide per la tutela della salute*, in "Diritto amministrativo", 2024, n. 4

I. Forgione (2022), *Il ruolo strategico dell'Agenzia nazionale per la cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna*, in "Diritto amministrativo", 2022, n. 4

J. Freund (2008), *La crisi dello Stato tra decisione e norma*, Guida, 2008

M.S. Giannini (1990), voce *Sovranità*, in "Enciclopedia del Diritto", Giuffrè, 1990

T. Giupponi (2024), *Il governo nazionale della cybersicurezza*, in "Quaderni costituzionali", 2024, n. 2

A. Iannuzzi (2024), *I regolamenti intersettoriali per l'istituzione dei "data spaces": Data Governance Act e Data Act*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi et al., "La regolazione europea della società digitale", Giappichelli, 2024

D.T. Khuel (2009), *From Cyberspace to Cyberpower: Defining the Problem*, in F.D. Kramer, S.H. Starr, L.K. Wentz (eds.), "Cyberpower and national security", University of Nebraska Press, 2009

D. King, R.C. Lieberman (2009), *Ironies of State Building: A Comparative Perspective on the American State*, in "World Politics", vol. 61, 2009, n. 3

M.C. Libicki (2009), *Cyberdeterrence and Cyberwar*, Rand Corporation, 2009

E. Longo (2024-a), *Il diritto costituzionale e la cybersicurezza. Analisi di un volto nuovo del potere*, in "Rassegna parlamentare", 2024, n. 2

E. Longo (2024-b), *Audizione informale per il disegno di legge in materia di "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" (AC 1717) Camera dei Deputati, Commissioni riunite I e II - Roma, 28 marzo 2024*, in "Rivista italiana di informatica e diritto", 2024, n. 1

E. Longo (2024-c), *La disciplina della cybersicurezza nell'Unione europea e in Italia*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi et al., "La regolazione europea della società digitale", Giappichelli, 2024

E. Longworth (2000), *The Possibilities for a Legal Framework for Cyberspace - including a New Zealand Perspective*, in T. Fuentes-Camacho (ed.), "The International Dimensions of Cyberspace Law", Unesco Publishing, 2000

W.J. Lynn III (2010), *Defending a New Domain: the Pentagon's Cyberstrategy*, in "Foreign Affairs", vol. 89, 2010, n, 5

D. Marrani (2021), *Il coordinamento delle politiche per la cybersecurity dell'UE nello spazio di libertà, sicurezza e giustizia*, in "Freedom, Security & Justice: European Legal Studies", 2021, n. 1

L. Martino (2018), *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in "Politica e società", 2018, n. 1

M. Matassa (2023), *La regolazione della cybersecurity in Italia*, in R. Ursi (a cura di), "La sicurezza nel cyberspazio", Franco Angeli, 2023

R. Mayntz (1999), *La teoria della governance: sfide e prospettive*, in "Rivista Italiana di Scienza Politica", 1999, n. 1

E.D. McCroskey, C.A. Mock (2017), *Operational Graphics for Cyberspace*, in "Joint Forces Quarterly", vol. 85, 2017

M. Mirti (2021), *Il cyberspace. Caratteri e riflessi sulla Comunità internazionale*, Edizioni Scientifiche Italiane, 2021

L. Moroni (2024), *La governance della cybersicurezza a livello interno ed europeo*, in "federalismi.it", 2024, n. 14

A. Negri (2011), *Sovereignity between government, exception and governance*, in H. Kalmo, Q. Skinner (eds.), "Sovereignty in Fragments. The Past, Present and Future of a Contested Concept", Cambridge University Press, 2011

R. Ottis, P. Lorents (2010), *Cyberspace: Definition and Implications, Proceeding of the International Conference on Information Warfare*, Cooperative Cyber Defense Centre of Excellence, 2010

P. Pătrașcu (2019), *Missions and Actions Specific to Cyberspace Operations*, in "Proceedings of the International Conference *Knowledge-based organization*", vol. 25, 2019, n. 3

L.R. Perfetti (2019), *L'organizzazione amministrativa come funzione della sovranità popolare*, in "Il diritto dell'economia", 2019, n. 1

M. Pietrangelo (2024), *La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo*, in "Rivista italiana di informatica e diritto", 2024, n. 2

B. Ponti (2024), *Il rapporto tra cybersicurezza e tutela dei dati personali: sinergie, bilanciamenti e parallelismi*, in "Rivista italiana di informatica e diritto", 2024, n. 2

L. Previti (2022), *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, in "federalismi.it", 2022, n. 25

R.A.W. Rhodes (1996), *The New Governance: Governing without government*, in "Political Studies", vol. 44, 1996

F.N. Ricotta (2024), Vulnerability disclosure *e* penetration testing*: profili giuridici rilevanti per l'adozione di una politica nazionale conforme alla Direttiva NIS 2*, in "Rivista italiana di informatica e diritto", 2024, n. 2

J. Rosenau, E.O. Czempiel (1992), *Governance without Government: Order and Change in World Politics*, Cambridge University Press, 1992

G.M. Ruotolo (2021), *Le fonti dell'ordinamento internazionale e la disciplina della Rete*, in "DPCE online", numero speciale, 2021

S.A. Salvaggio (2023), *The European framework for cybersecurity: strong assets, intricate history*, in "International Cybersecurity Law Review", vol. 4, 2023

M. Santaniello (2022), *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, in "Rivista italiana di informatica e diritto", 2022, n. 1

F. Serini (2022), *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in "federalismi.it", 2022, n. 12

E. Sorrentino, A.F. Spagnuolo (2024), *Cybersecurity e sovranità digitale nella protezione dei dati personali*, in "Rivista italiana di informatica e diritto", 2024, n. 2

S. Tagliagambe (1997), *Epistemologia del cyberspazio*, Demos, 1997

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

F. Zorzi Giustiniani (2021), *Il* Position Paper *dell'Italia sull'applicabilità del diritto internazionale nel cyberspazio, la sentenza del Tribunale UE nel caso Google Shopping e l'Oxford Statement sulla regolamentazione internazionale degli attacchi* ransomware, in "Nomos. Le attualità del diritto", 2021, n. 3

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0246 • articolo sottoposto a peer review • pubblicato in anteprima il 20 nov. 2025

Indra Macrì

Dati pubblici di qualità per la crescita del Paese

Il contributo descrive la disciplina in materia di dati aperti e di riutilizzo dell'informazione pubblica, che rappresentano il carburante dell'intelligenza artificiale e uno dei pilastri della strategia europea in materia di dati. Si analizzano le caratteristiche dei dati aperti sotto il profilo tecnico, economico oltre che le condizioni per il riutilizzo e le licenze d'uso. Si approfondisce l'ambito di applicazione, sia con riferimento ai soggetti chiamati all'attuazione della direttiva europea, sia con riguardo ai dati oggetto di riutilizzo. Si fornisce una lettura incrociata con la regolamentazione secondaria, evidenziando i nuovi obblighi di transizione digitale introdotti per il riutilizzo dei dati aperti. Si illustrano le specificità definite dal legislatore per il riutilizzo dei dati dinamici e dei dati della ricerca, oltre che i dati di elevato valore e il relativo regolamento di esecuzione.

Dati aperti – Riutilizzo dei dati pubblici – Strategia europea sui dati – Obblighi di transizione digitale

Quality public data for the growth of the country

The paper describes the legislation on open data and re-use of public sector information, which represent the fuel of artificial intelligence and one of the pillars of European data strategy. The characteristics of open data are analyzed from a technical and economic point of view as well as the conditions for reuse and licenses for use. The scope of application is explored in depth, with reference to the subjects called upon to implement the European directive and with regard to the data subject to reuse. A cross-reading with secondary regulation is provided, highlighting the new digital transition obligations introduced for the reuse of open data. The specificities defined by the legislator for the reuse of dynamic data and research data, as well as high-value data and related implementing regulation, are illustrated.

Open data – Re-use of public sector information – European data strategy – Digital transition obligations

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

1. Introduzione

La Commissione europea sottolinea in molteplici comunicazioni come tutti i cittadini dovrebbero avere la possibilità di prendere decisioni migliori sulla base delle informazioni derivate dai dati, che dovrebbero essere accessibili a tutti gli attori, pubblici o privati, grandi o piccoli, start-up o mega imprese. Da diversi anni, secondo la Commissione europea, una serie di fattori, fra i quali l'apertura dei dati, consente alla società di trarre il massimo vantaggio dall'innovazione e dalla concorrenza, garantendo a tutti "un dividendo digitale"[1]. Proprio l'impatto economico prodotto dall'innovazione digitale ha indotto le istituzioni europee a concentrarsi con diversi provvedimenti su specifici temi, fra i quali l'apertura dei dati, che hanno avuto e continuano ad avere una crescente rilevanza nell'attività della pubblica amministrazione. L'espressione "apertura dei dati" traduce quella inglese "open data", talvolta resa anche con la locuzione "dati aperti", che non ha a che fare esclusivamente con la loro conoscibilità da parte di tutti, ma ha anche, e soprattutto, una precisa connotazione tecnica come approfondito più avanti. Negli anni passati, tuttavia, i dati aperti, in Italia, sono stati visti essenzialmente come lo strumento per la realizzazione della "casa di vetro", ossia di quell'amministrazione che nulla avrebbe dovuto celare ai suoi cittadini. Si riteneva che una pubblica amministrazione trasparente avrebbe dovuto aprire i propri dati, nel senso di renderli conoscibili a chiunque. Ma per garantire la trasparenza occorre che i dati pubblicati siano intellegibili da qualsiasi persona, non da qualsiasi macchina. Mentre, invece, fra le caratteristiche tecniche principali dei dati aperti vi è la capacità di essere letti in modo automatico, *machine readable*. Ciò implica che i dati aperti, in quanto tali, sono rappresentati attraverso formati adatti ad un'elaborazione automatica, che non si conciliano con gli obiettivi di trasparenza, intesa come immediata fruizione da parte del soggetto interessato a quell'informazione. La fruizione di un dato aperto, infatti, difficilmente risulta istantanea e agevole per una persona, in quanto richiede un opportuno programma di elaborazione per la lettura dello specifico formato nel quale il dato è stato rappresentato. Come chiarito nello stesso titolo della direttiva europea 2019/1024 sugli *open data* l'obiettivo della disciplina in materia di apertura dei dati consiste nel riutilizzo delle informazioni, ossia nell'uso dei dati che sono stati resi aperti per altre finalità, per un uso nuovo, differente, appunto un "ri-uso". A tal riguardo, però, occorre una precisazione sui termini riutilizzo e riuso, a volte adoperati come sinonimi, pur avendo significati leggermente differenti. Nel linguaggio comune con la parola "riuso" si intende – in contrapposizione a nuovo – qualcosa in precedenza posseduto

1. Commissione europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Plasmare il futuro digitale dell'Europa*, 19 febbraio 2020, doc. COM(2020) 67.

da altri, che viene adoperato in una fase successiva; il termine riutilizzo, invece, contiene al suo interno anche il concetto della "utilità", ossia di una nuova applicazione di un oggetto che può risultare funzionale a fini diversi rispetto a quelli iniziali per i quali era stato inizialmente predisposto. La differenza fra i due termini "riutilizzo" e "riuso", sopra richiamata, è annullata nella lingua inglese, dove il termine adoperato per indicare il riutilizzo dell'informazione pubblica è appunto *re-use of public sector information*, così accentuando la percezione di equivalenza anche nella lingua italiana dei due termini. La normativa italiana di settore, tuttavia, nell'impiego dei due termini, "riuso" e "riutilizzo", opera una distinzione: il "riuso" fa riferimento al software, mentre il "riutilizzo" riguarda i dati delle pubbliche amministrazioni ed esclude (nel nostro Paese) espressamente il software. Il riuso viene effettuato dalla pubblica amministrazione ed ha per oggetto il software sviluppato da (o per) altre pubbliche amministrazioni, in attuazione dell'art. 69 del Codice dell'amministrazione digitale (Cad, d.lgs. 7 marzo 2025, n. 82). Il riutilizzo, invece, non può essere esercitato da un ente pubblico, come meglio chiarito nel prosieguo, ma solo da un soggetto privato ed ha per oggetto dati (e non software!) dei quali è titolare una pubblica amministrazione.

2. Dati per la crescita economica

La strategia europea sui dati già nel 2020 mette in evidenza come il costante incremento della quantità di dati richieda che la metodologia di raccolta e utilizzo di tali dati tenga conto anzitutto degli interessi delle persone, conformemente ai valori, ai diritti fondamentali e alle norme europee. Molta dell'attenzione converge, in particolare, sul volume crescente di dati industriali non personali, come ad esempio le informazioni prodotte dai sensori di apparati elettronici, e di dati pubblici, ossia i dati prodotti da istituzioni e che sono oggetto di pubblicazione. Tali aspetti, insieme ai cambiamenti tecnologici in materia di conservazione ed elaborazione dei dati, secondo l'Europa, costituiscono una potenziale fonte di crescita e innovazione da sfruttare, oltre che l'occasione per cittadini e imprese di prendere decisioni migliori basate sui dati[2]. In queste nuove sfide che l'Europa affronta per la crescita della sua competitività economica nel contesto globale, i dati delle pubbliche amministrazioni italiane hanno un ruolo chiave. Per questo motivo le istituzioni pubbliche sono le protagoniste di alcuni dei provvedimenti che riguardano la produzione di dati di qualità e la loro messa a disposizione.

Con le direttive sul riutilizzo dei dati[3] l'Europa da diversi anni intende disciplinare la materia dei dati pubblici al servizio di tutti. L'ultima direttiva del 2019 sull'apertura dei dati e sul riutilizzo dell'informazione pubblica, in particolare, si focalizza sui "dati aperti" (o *open data*) e fornisce molteplici indicazioni ai soggetti pubblici per consentire il più ampio riutilizzo dei dati da parte di soggetti privati, cittadini o imprese per fini commerciali o non commerciali. Se è vero che la prima direttiva in materia è del 2003, soltanto con il recente Regolamento di esecuzione del 2023[4], l'Europa si concentra su specifiche tipologie di dati, le cosiddette serie di dati di elevato valore, definendo regole tecniche comuni che abbracciano l'intero ciclo di vita del dato: dalla sua creazione alla sua messa a disposizione. Per creare valore attraverso i dati, infatti, consentendone il più ampio riutilizzo, occorre che siano definite *ex-ante* le modalità di raccolta e rappresentazione delle informazioni.

Nell'attuale contesto di sviluppo dominato dall'intelligenza artificiale, i dati e la loro "qualità" acquistano maggiore valore, perché rappresentano il carburante raffinato che alimenta la stessa intelligenza artificiale. Al riguardo, le istituzioni europee nel rappresentare i contenuti della strategia

2. Commissione europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Una strategia europea per i dati*, 19 febbraio 2020, doc. COM(2020) 66, p. 1.
3. Direttiva (UE) 2019/1024 del Parlamento Europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (rifusione della precedente Direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, relativa al riutilizzo dell'informazione del settore pubblico).
4. Regolamento di esecuzione (UE) 2023/138 della Commissione, del 21 dicembre 2022, che stabilisce un elenco di specifiche serie di dati di elevato valore e le relative modalità di pubblicazione e riutilizzo.

sui dati[5], citano gli studi Draghi e Letta sul futuro della crescita del mercato e della competitività. Lo sviluppo economico è legato alla capacità di competere, che, a sua volta, dipende anche da come si riuscirà a trarre valore dall'intelligenza artificiale e, quindi, dai dati. Si prevede, in particolare, che coloro i quali possano liberamente accedere a nuove ricerche, dati sempre più accurati e tecnologie più efficienti possono innovare più rapidamente, migliorare i loro processi e mantenere la competitività nel mercato globale[6]. L'Europa, secondo lo studio, dovrebbe promuovere un coordinamento interindustriale e una condivisione dei dati per accelerare l'integrazione dell'intelligenza artificiale nell'industria europea[7]. Anche in risposta a queste sollecitazioni, l'Unione europea ha recentemente adottato una comunicazione, *AI Continent Action Plan*, dichiarando il proprio impegno e la propria determinazione a diventare un leader globale nel campo dell'intelligenza artificiale per ottenere un'economia più forte, innovazioni nel settore sanitario, nuovi posti di lavoro, maggiore produttività, migliori trasporti e istruzione, una maggiore protezione contro le minacce informatiche e supporto nella lotta ai cambiamenti climatici. Il Piano d'azione per l'intelligenza artificiale del Continente, nel quale si annuncia l'adozione di una nuova strategia dell'Unione europea in materia di dati, mira a promuovere e accelerare le politiche europee in sinergia con gli Stati membri. Il piano si articola su cinque aree chiave: investimento in infrastrutture di calcolo su larga scala, miglioramento dell'accesso ai dati, sviluppo di algoritmi di intelligenza artificiale e loro diffusione, rafforzamento delle competenze, promozione della conformità normativa, favorendone la semplificazione[8]. L'impegno dell'Europa per lo sviluppo dell'intelligenza artificiale è continuo, come dimostrato dai lavori del vertice dello scorso giugno sul digitale svoltosi a Danzica, dove, fra l'altro, è stata annunciata la strategia *IA Apply Strategy*. La strategia, adottata lo scorso 8 ottobre 2025, introduce per imprese e settore pubblico il principio *AI first policy*, con il quale si incoraggia ad integrare l'intelligenza artificiale basandosi sulle soluzioni europee[9].

3. Disciplina in materia di apertura dei dati e riutilizzo dell'informazione pubblica

La prima versione della direttiva del 2003 relativa al riutilizzo delle informazioni del settore pubblico[10] individuava fra le finalità quella di consentire alle imprese europee di sfruttarne il potenziale, così contribuendo alla crescita economica e alla creazione di posti di lavoro. Nella prima versione, quindi la direttiva sul riutilizzo dell'informazione pubblica non annoverava fra le sue mire in modo espresso anche la trasparenza. Le modifiche operate nel 2013[11] e la successiva versione del 2019, nel riprendere gli stessi obiettivi della direttiva del

5. Data Europa Academy, webinar *Navigating the European data strategy. The progress towards the single market of data*, 31 gennaio 2025.
6. E. Letta, *Much more than a market – Speed, Security, Solidarity Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens*, aprile 2024, p. 22.
7. "*The Draghi report: A competitiveness strategy for Europe (Part A)*", p. 34.
8. European Commission, Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the regions "AI Continent Action Plan", 9 aprile 2025, doc. COM(2025) 165.
9. European Commission, Communication from the Commission to the European Parliament and the Council "Apply AI Strategy", 8 ottobre 2025, doc. COM(2025) 724.
10. La direttiva 2003/98/CE del Parlamento europeo e del Consiglio del 17 novembre 2003, relativa al riutilizzo dell'informazione del settore pubblico, originariamente non trattava anche dell'apertura dei dati.
11. Nel considerando 4 della direttiva 2013/37/UE del Parlamento europeo e del Consiglio del 26 giugno 2013 che modifica la direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico si indica come la "possibilità di riutilizzare i documenti detenuti da un ente pubblico conferisce un valore aggiunto per i riutilizzatori, gli utenti finali e la società in generale e, in molti casi, per lo stesso ente pubblico, grazie alla promozione della trasparenza e della responsabilizzazione e al ritorno di informazione fornito dai riutilizzatori e dagli utenti finali che permette all'ente pubblico in questione di migliorare la qualità dei dati che raccoglie".

2003, in più sembrano volersi adeguare alla spinta del movimento per gli *open data* e prevedono fra le loro finalità, fra l'altro, anche importanti obiettivi sociali quali la responsabilizzazione e la trasparenza, osservando come il riutilizzo non solo conferisce un valore aggiunto per i riutilizzatori, gli utenti finali e la società in generale, ma, in diversi casi, per la stessa PA promuovendone la trasparenza e la responsabilizzazione. Un altro elemento di vantaggio per l'ente pubblico consiste nei feedback che lo stesso può ricevere dai riutilizzatori dell'informazione della quale l'ente è titolare. Al riguardo, la modifica del 2013 ravvede un ulteriore vantaggio per l'ente pubblico, ossia il miglioramento della qualità dei dati che raccoglie, al quale la versione del 2019 aggiunge anche il miglioramento dell'"adempimento dei propri compiti".

L'adozione del paradigma dei dati aperti nella pubblica amministrazione, quindi, non costituisce soltanto la risposta all'adempimento delle istituzioni in materia di riutilizzo, ma, una volta che il riutilizzo dell'informazione pubblica opera, questo produce come corollario la promozione anche della trasparenza, della partecipazione e della collaborazione, arrivando a generare vantaggi per lo stesso ente pubblico, individuati dal legislatore europeo nella qualità dei dati, oltre che nell'adempimento stesso dei propri compiti istituzionali.

Il tema dei dati e del riutilizzo dell'informazione pubblica, sia per la grande mole di dati prodotti e la necessità di gestirli secondo precisi standard (ad esempio, nell'ambito della ricerca), sia per gli aspetti di sicurezza e, più di recente, per i risvolti nell'applicazione dell'intelligenza artificiale, sia per il necessario impatto sull'innovazione delle pubbliche amministrazioni, nel corso degli anni è stato trattato da molti autori sotto diversi profili[12]. Come osservato, la nozione di dato aperto è racchiusa in una disciplina diversa da quella dedicata all'accesso[13]. In Italia, la disponibilità dei dati aperti è stata vista, essenzialmente, in funzione della trasparenza amministrativa, diversamente da quanto avvenuto negli Stati Uniti dove prevale l'aspetto economico, in quanto l'apertura dei dati è funzionale al loro sfruttamento per scopi commerciali[14].

Da circa vent'anni la direttiva 2003/98/CE del 17 novembre 2003 relativa al riutilizzo dell'informazione del settore pubblico ha stabilito che le pubbliche amministrazioni titolari di dati pubblici ne consentono il riutilizzo da parte dei soggetti che ne abbiano bisogno per proprie finalità. Come espressamente previsto dal d.lgs. 24 gennaio 2006,

12. Si veda, fra gli altri, Aliprandi 2011; Calzolaio 2016; Carloni 2022; Carullo 2025; Cascione 2005; Costantino–Maddalena 2023; D'Orlando–Orsoni 2019; Galetta 2019; Mancosu 2019; Mancosu 2016; Martignago 2022; Monica 2024; Pagnanelli 2021; Patrito–Pavoni 2012; Pietrangelo 2004; Ponti 2006; Sciacchitano 2018; Sganga 2022; Spagnuolo–Sorrentino 2022; Strazza 2022; Wilkinson–Dumontier–Aalbersberg et al. 2016.

13. Strazza 2022: l'autrice, al riguardo, osserva che "il tema degli open data è spesso confuso con quello della trasparenza, con cui è strettamente connesso, ma non del tutto sovrapponibile", segnalando come la "equivoca riducibilità dell'apertura dei dati alla (sola) trasparenza amministrativa ha offuscato, però, le potenzialità del riuso per fini commerciali degli open data (aspetto spesso trascurato dalle stesse P.A.)".

14. Galetta 2019: la stessa autrice, al riguardo, osserva come "nel panorama dottrinario italiano, l'idea che emerge è che si debba ottenere l'accesso ai dati in possesso delle Istituzioni Pubbliche, liberi da limitazioni tecnologiche e legali che ne impediscano il riuso, la modifica e la combinazione con altri dati, allo scopo di 'accedere alle informazioni in maniera molto diretta e trasparente, per renderci cittadini più consapevoli e dunque più liberi'. Sicché il tema risulta, sin dal principio, essenzialmente connesso – potremmo dire, addirittura, confuso – col più ampio tema della trasparenza". La stessa autrice, richiamando l'art. 53 comma 1-*bis*, del d.lgs. n. 82/2005 che, dispone, ai sensi dell'articolo 9 del decreto trasparenza (d.lgs. n. 33/2013), la pubblicazione anche "(de)l catalogo dei dati e dei metadati , nonché delle relative banche dati in loro possesso e i regolamenti che disciplinano l'esercizio della facoltà di accesso telematico e il riutilizzo di tali dati e metadati›", introdotto dall'art. 43, c. 1, lett. c), d.lgs. n. 179/2016, afferma che il nostro Cad, non a caso, obbliga le amministrazioni alla pubblicazione dei dati coerentemente con la normativa sulla trasparenza. Con ciò l'autrice lascia intendere come il rinvio del Codice dell'amministrazione digitale alla disciplina sulla trasparenza per quanto attiene al riutilizzo dell'informazione pubblica abbia creato un legame fra queste due tematiche inducendo la dottrina a trattare le due materie in continuità.

n. 36 di recepimento della succitata direttiva europea, titolare del dato è l'amministrazione o l'organismo di diritto pubblico che ha originariamente formato il dato, o che ha commissionato ad altro soggetto pubblico o privato il documento che lo rappresenta, o che ne ha la disponibilità (art. 2, comma 1, lett. i). Ad esempio, l'Università è titolare dei dati relativi ai diplomi di laurea che rilascia (disciplina di laurea, voto, data di conseguimento, ecc.), poiché si tratta di dati originariamente formati dalla stessa Università. Il Ministero dell'economia e delle finanze è titolare dei dati relativi al patrimonio pubblico, avendone commissionato la raccolta attraverso apposita banca dati (ossia "il documento che lo rappresenta") al proprio partner tecnologico, che è la Sogei S.p.A. L'Agenzia per l'Italia digitale è titolare dell'Indice delle pubbliche amministrazioni, IPA, in quanto ha la disponibilità dei dati delle pubbliche amministrazioni relativi ad esempio, ai domicili digitali, al responsabile dei sistemi informativi, ecc.

L'obiettivo sotteso alla norma, come sopra richiamato, è lo sviluppo del mercato dei dati e il loro libero utilizzo, che produce, secondo le istituzioni europee, la possibilità per le imprese europee di sfruttare il potenziale dei dati e di contribuire alla crescita economica e, quindi, alla creazione di posti di lavoro. Il decreto di recepimento della direttiva, d.lgs. n. 36/2006, nella sua originaria versione non stabiliva un obbligo in capo alle pubbliche amministrazioni di mettere a disposizione i propri dati per il riutilizzo. Al contrario. La prima versione del d.lgs. n. 36/2006 stabiliva che le "pubbliche amministrazioni e gli organismi di diritto pubblico non hanno l'obbligo di consentire il riutilizzo dei documenti" contenenti dati pubblici che sono nella loro disponibilità (art. 1, comma 2). L'attuazione della direttiva, quindi, nella sua prima stesura, non ha prodotto i risultati attesi, essendosi creata un'ambiguità di fondo, come sottolineato dalla dottrina[15]. Il legislatore europeo con la nuova direttiva 2019/1024 abroga la precedente, concentrandosi non solo sul riutilizzo dell'informazione del settore pubblico, ma, *in primis* sull'apertura dei dati.

Come meglio chiarito di seguito, l'apertura dei dati costituisce, infatti, la condizione imprescindibile per esercitarne il riutilizzo. Tanto il legislatore europeo nella direttiva, quanto quello italiano nel decreto di recepimento della stessa, stabiliscono che per "riutilizzo" si intende "l'uso, da parte di persone fisiche o giuridiche, di documenti in possesso di: a) enti pubblici a fini commerciali o non commerciali diversi dallo scopo iniziale nell'ambito dei compiti di servizio pubblico per i quali i documenti sono stati prodotti, fatta eccezione per lo scambio

15. Ponti 2006 ha osservato come "il dato testuale definisce esplicitamente 'la decisione di consentire o meno il riutilizzo' da parte dell'amministrazione in termini di 'potere'. Rispetto a questa perentoria indicazione, il decreto non offre però indizi sicuri in ordine alla identificazione della natura di questo 'potere'. Il suo esercizio, infatti, è finalizzato a rendere disponibile per il riutilizzo il maggior numero di informazioni, ciò che deporrebbe per una lettura in termini di un potere-dovere di natura pubblicistica, funzionale alla realizzazione di un interesse pubblico. Tuttavia, una serie di ulteriori elementi sembrano smentire tale ipotesi, a cominciare dalla mancata previsione del dovere di motivare la decisione negativa a fronte di una richiesta di riutilizzo, e degli strumenti di ricorso (in via amministrativa) avverso tale diniego. Di più, nella misura in cui la decisione appare integralmente rimessa all'amministrazione, essa sembra atteggiarsi alla stregua di un potere sostanzialmente privatistico, non diverso da quello che ha ogni detentore di un bene che interessa potenziali acquirenti, e che può scegliere se metterlo o meno a loro disposizione. Depongono in questo senso sia la disciplina sostanziale del riutilizzo, laddove l'amministrazione è riguardata alla stregua di un monopolista dell'informazione del settore pubblico (…), sia i criteri di tariffazione, che nel caso di riutilizzo a fini commerciali tendono ad assicurare comunque un utile all'amministrazione cedente (…). È di tutta evidenza che questa profonda ambiguità circa la natura del potere di concedere le informazioni a fini di riutilizzo comporta delle conseguenze profondamente differenziate quanto al regime del riutilizzo, a cominciare dalla applicabilità o meno della disciplina del procedimento amministrativo alle attività poste in essere dall'amministrazione a seguito della richiesta di messa a disposizione delle informazioni da parte dei soggetti interessati al riutilizzo, ovvero quanto al tipo di tutela giuridica cui può aspirare tale pretesa. Si aggiunga, poi, che il differente criterio di tariffazione previsto, a seconda che le attività di riutilizzo perseguano o meno finalità commerciali, contribuisce ad aggravare ulteriormente tale ambiguità di fondo".

di documenti tra enti pubblici esclusivamente in adempimento dei loro compiti di servizio pubblico; b) imprese pubbliche a fini commerciali o non commerciali diversi dallo scopo iniziale di fornire i servizi di interesse generale per i quali i documenti sono stati prodotti, fatta eccezione per lo scambio di documenti tra imprese pubbliche ed enti pubblici esclusivamente in adempimento dei compiti di servizio pubblico degli enti pubblici" (art. 2, punto 11) dir. 2019/1024, ripreso anche dall'art. 2, lett. e), d.lgs. n. 36/2006). La definizione espressamente esclude, quindi, lo "scambio di documenti" fra soggetti pubblici, che rappresenta una fattispecie distinta rispetto al riutilizzo. Per potersi configurare un "riutilizzo" di dati, come inteso dalla normativa sopra richiamata, quindi, sembrerebbe necessario il verificarsi in contemporanea di determinate condizioni relative alla titolarità del dato, al soggetto che lo riutilizza e allo scopo, ossia:

1) Titolarità del dato. I dati dovranno essere nella disponibilità di una pubblica amministrazione o di un'impresa pubblica, come individuata dall'ambito di applicazione della direttiva. I dati detenuti da un privato, infatti, non possono essere oggetto di riutilizzo ai sensi della dir. 2019/1024;
2) Soggetto che riutilizza il dato. Occorre la presenza di un soggetto non pubblico interessato a quei dati. Nell'ipotesi, infatti, che sia un soggetto pubblico ad aver bisogno del dato di un'altra amministrazione per lo svolgimento della propria attività istituzionale, procederà allo "scambio" del dato e non al suo "riutilizzo";
3) Scopo del riutilizzo. Lo sfruttamento dei dati avviene per fini commerciali o non commerciali, in ogni caso per fini differenti da quelli iniziali per i quali i dati erano stati raccolti[16].

Quando l'amministrazione si pone l'obiettivo di pubblicità e trasparenza, poiché, spesso, gli open data non sono idonei a consentire una effettiva conoscenza e comprensione, è richiesta una "ri-elaborazione" dell'informazione. Ci si potrebbe chiedere se tale operazione, ossia la rielaborazione di dati aperti, possa rappresentare un esempio di "riutilizzo". Si pensi, ad esempio, al caso concreto del bilancio di un ente pubblico. Per motivi di trasparenza tale bilancio è soggetto a pubblicazione. Il d.lgs. n. 33/2013 stabilisce, in particolare, che le pubbliche amministrazioni pubblicano e rendono accessibili, "i dati relativi alle entrate e alla spesa di cui ai propri bilanci preventivi e consuntivi in formato tabellare aperto che ne consenta l'esportazione, il trattamento e il riutilizzo". La stessa norma esplicita altresì che tale pubblicazione avviene secondo uno schema tipo e modalità individuati con decreto del Presidente del Consiglio dei ministri – adottato il 22 settembre 2014 – dove si definiscono gli schemi e le modalità per la pubblicazione su Internet dei dati relativi alle entrate e alla spesa dei bilanci preventivi e consuntivi e l'indicatore annuale di tempestività dei pagamenti delle pubbliche amministrazioni (art. 29, comma 1-bis, d.lgs. n. 33/2013). Cosicché l'obiettivo di trasparenza dei documenti di bilancio è assolto da parte delle pubbliche amministrazioni con la produzione – e successiva pubblicazione sul sito Internet – di un file pdf che riporta i singoli valori contabili in corrispondenza di ciascuna delle voci individuate dagli schemi di bilancio definiti dal citato decreto. Si badi bene, però, pur essendo il pdf un formato aperto e pienamente rispondente all'obiettivo di

16. In tal senso anche il Consiglio di Stato ha stabilito che non può parlarsi di riutilizzo laddove "l'amministrazione provinciale (…) si limita a gestire il servizio di accesso ai dati del libro fondiario nei limiti della potestà autoritativa attribuita per fini istituzionali alla stessa dal legislatore, [in quanto] difetta ontologicamente quell'uso dei dati per fini diversi che rappresenta il presupposto logico-giuridico per l'applicazione della disciplina sul riutilizzo" (sentenza n. 00485/2023). Nella stessa sentenza e nella successiva sentenza n. 00487/2023 i giudici di Palazzo Spada riprendono il testo del considerando 8 della direttiva n. 2003/98 (*ratione temporis* applicabile), secondo il quale: "Affinché il riutilizzo dei documenti del settore pubblico avvenga in condizioni eque, adeguate e non discriminatorie, le modalità di tale riutilizzo devono essere soggette ad una disciplina generale. Gli enti pubblici raccolgono, producono, riproducono e diffondono documenti in adempimento dei loro compiti di servizio pubblico. L'uso di tali documenti per altri motivi costituisce riutilizzo". Le stesse indicazioni sono state identicamente trasposte nel considerando 20 della direttiva n. 1024/2019 che abroga la direttiva n. 2003/98. Il Consiglio di Stato, in sintesi, sottolinea l'essenzialità della presenza di uno scopo differente da quello iniziale per il quale i dati erano stati originariamente prodotti per potersi configurare un riutilizzo.

trasparenza, esso non rappresenta la scelta più adeguata per assolvere anche agli obiettivi di "scambio" e di "riutilizzo" dell'informazione. Tale formato, infatti, non consente una lettura automatica del dato e, conseguentemente, impedisce l'esecuzione di operazioni sui valori indicati per ciascuna delle voci degli schemi di bilancio. Il successivo decreto legislativo 25 maggio 2016, n. 97[17] interviene con l'art. 9 sul tema, indicando alle amministrazioni una strada alternativa ed esemplificativa per ottemperare agli obblighi di trasparenza in materia contabile, ossia la trasmissione dei bilanci alla Banca dati delle amministrazioni pubbliche (BDAP), istituita dall'articolo 13 della legge del 31 dicembre 2009, n. 196 di contabilità e finanza pubblica. Nel frattempo, il decreto 12 maggio 2016 del Ministero dell'economia e delle finanze[18] aveva stabilito che le amministrazioni predispongono in formato aperto XBRL i loro bilanci e lo trasmettono alla BDAP. Tale dato, ossia il bilancio elaborato in XBRL, poiché si tratta di un formato dati aperto e *machine readable* non consentirebbe un'immediata fruizione dell'informazione, se non intervenisse una ri-elaborazione del bilancio per il tramite del portale OpenBDAP (dove, ad esempio, vi sono aggregazione delle voci, in una semplificazione dei dati a fini di leggibilità, nel confronto con gli esercizi precedenti) gestito dal Dipartimento della Ragioneria generale dello Stato (RGS). In questo caso, ci si chiede se sia possibile parlare *tout court* di "riutilizzo" del dato. Nell'esempio illustrato la ri-elaborazione è effettuata da una pubblica amministrazione (la RGS) per le finalità istituzionali individuate dalla disposizione sopra richiamata della legge di contabilità e finanza pubblica. Sembrerebbe, quindi, venir meno la condizione 2), prima enucleata, secondo la quale il riutilizzo può essere esercitato da un privato e non una pubblica amministrazione nello svolgimento delle proprie attività istituzionali. Fino a poco fa anche Open Polis rielaborava proprio i dati di bilancio delle pubbliche amministrazioni. Open Polis risulta una fondazione e nell'elaborazione dei dati di bilancio soddisfa senz'altro la condizione 1) e 2) sul riutilizzo dei dati, operando, in quanto soggetto privato (condizione 2), una rielaborazione di dati detenuti da amministrazioni pubbliche (condizione 1). Dal sito di Open Polis si apprende che fra le finalità delle loro iniziative vi sono l'accesso alle informazioni pubbliche, la trasparenza e la partecipazione democratica. In questo caso ci si potrebbe porre il problema di comprendere se la rielaborazione dei dati di bilancio da parte di Open Polis soddisfi anche la condizione 3), relativa allo scopo del riutilizzo. Affinché si concretizzi il riutilizzo occorre che vi siano fini commerciali o non, ma comunque "diversi" da quelli iniziali nell'ambito dei compiti di servizio pubblico per i quali i documenti erano stati originariamente prodotti. Se i documenti di bilancio vengono visti come un documento di rendicontazione economica, finanziaria e patrimoniale, quindi sono redatti con l'obiettivo di "rendere conto" ai cittadini delle entrate, delle spese e della situazione patrimoniale, ecco che la loro principale finalità è quella della trasparenza nell'uso delle risorse da parte del singolo ente pubblico. Letta sotto questo profilo, quindi, ci si chiede se l'operazione di Open polis soddisfi la condizione 3) sulle finalità del riutilizzo, in quanto anche l'Amministrazione si pone il medesimo obiettivo di trasparenza nella redazione del bilancio. In altri termini può parlarsi di riutilizzo se nella sua rielaborazione il privato intende raggiungere gli stessi obiettivi di trasparenza che si prefigge l'ente pubblico? Una ulteriore lettura sarebbe, tuttavia, possibile. Le pubbliche amministrazioni, in coerenza con l'ordinamento dell'Unione europea, assicurano l'equilibrio dei bilanci e la sostenibilità del debito pubblico (art. 97, Cost.). A tal fine redigono i loro bilanci, che rappresentano lo strumento attraverso il quale le diverse istituzioni (ad esempio Ministero dell'economia e delle finanze, Corte dei conti) esercitano il controllo e monitoraggio del rispetto degli equilibri di bilancio. Se la funzione di controllo e monitoraggio prevalesse, allora sarebbe possibile concludere che quello operato da Open Polis sui

17. D.lgs. n. 97/2016 di revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124 sulla riorganizzazione delle amministrazioni pubbliche.
18. Decreto 12 maggio 2016 del Ministero dell'economia e delle finanze, *Modalità di trasmissione dei bilanci e dei dati contabili degli enti territoriali e dei loro organismi ed enti strumentali alla banca dati delle pubbliche amministrazioni,* pubblicato in Gazzetta Ufficiale n. 122 del 26 maggio 2016.

dati di bilancio costituisce un effettivo "riutilizzo". La rielaborazione dei bilanci delle pubbliche amministrazioni da parte di Open polis, infatti, andrebbe a soddisfare anche la terza condizione relativa alla "diversa finalità", ossia la "trasparenza", che, nell'ipotesi formulata, risulterebbe differente dalla finalità di "controllo e monitoraggio" per la quale il dato contabile in questione era stato originariamente prodotto.

Certamente i dati aperti contribuiscono all'obiettivo di riutilizzo, come meglio discusso in seguito, ma allo stesso tempo con l'art. 7 del d.lgs. n. 33/2013 il legislatore italiano sembra abbia voluto loro assegnare anche il delicato compito di realizzare gli obiettivi di pubblicità, stabilendo che i documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria, resi disponibili anche a seguito dell'accesso civico, sono pubblicati in formato di tipo aperto[19] e sono riutilizzabili ai sensi del decreto legislativo 24 gennaio 2006, n. 36, del decreto legislativo 7 marzo 2005, n. 82, e del decreto legislativo 30 giugno 2003, n. 196, senza ulteriori restrizioni diverse dall'obbligo di citare la fonte e di rispettarne l'integrità. Anche se la rubrica dell'art. 7 del d.lgs. n. 33/2013 è "Dati aperti e riutilizzo", nel testo dell'art. 7 ci si riferisce al formato aperto (*open format*), piuttosto che a dati di tipo aperto (*open data*). Il formato caratterizza sotto il profilo tecnico i dati aperti, cosicché un dato aperto deve essere rappresentato in formato aperto, ma non tutti i dati in formato aperto sono dati aperti (*open data*)[20]. Con ciò è possibile concludere che tutti i dati che sono oggetto di accesso civico, hanno caratteristiche tecniche (il formato aperto), che li rende candidabili a essere resi disponibili ai fini del riutilizzo. La correlazione fra l'accesso civico e il riutilizzo dei dati pubblici non produce, però, una sovrapposizione fra le due discipline. Al contrario, una recente sentenza della Corte di giustizia dell'Unione europea ha tracciato una marcata distinzione fra i due istituti, affermando che se "è vero che il 'riutilizzo', ai sensi della direttiva 2019/1024, presuppone l'accesso ai documenti […], ciò non toglie che si tratta di due operazioni manifestamente distinte". La CGUE, infatti, ha stabilito che "la direttiva 2019/1024 deve essere interpretata nel senso che una richiesta di accesso a documenti in possesso di un ente pubblico non rientra nel suo ambito di applicazione"[21]. Dal ché sembrerebbe possibile dedurre che seppure le amministrazioni pubbliche siano tenute alla predisposizione dei loro dati in formato aperto per consentirne il riutilizzo, ciò non implica che esse debbano produrre questi dati ai fini dell'accesso, poiché quest'ultimo non rientra nell'ambito di applicazione della dir. 2019/1024 e, quindi, del d.lgs. n. 36/2006.

3.1. Dati e documenti

Prima di procedere con i successivi approfondimenti, occorre chiarire che per documento si intende "la rappresentazione di atti, fatti e dati a prescindere dal supporto, cartaceo o elettronico, registrazione sonora, visiva o audiovisiva o qualsiasi parte di tale contenuto nella disponibilità della pubblica amministrazione o dell'organismo di diritto pubblico" (art. 2, comma 1, lett. c), d.lgs. n. 36/2006). Tale definizione, già presente da tempo nella normativa italiana, richiama quella della corrispondente direttiva 2019/1024, che, in più, rispetto alla definizione indicata dal nostro legislatore italiano, precisa che è da intendersi "documento" anche la *raccolta* di dati, fatti o informazioni (considerando 30). Cosicché un archivio, inteso come raccolta di dati e/o informazioni, sia esso cartaceo o digitale, è da considerarsi un documento secondo le indicazioni contenute nella direttiva, che nei fatti utilizza il termine generico "documento", come "metonimia", perché espressamente stabilisce che la definizione di documento comprende qualsiasi parte di esso o aggregazione di più documenti o dati. La direttiva, inoltre, lascia al singolo Stato membro la possibilità di includere

19. Il testo letterale dell'articolo precisa "ai sensi dell'articolo 68 del Codice dell'amministrazione digitale". Tale rinvio, però, tenuto conto delle novelle intervenute sul Cad nel 2017, è oggi da riferirsi all'art. 1, comma 1, lett. l-*bis*), che riporta la definizione di formato aperto. La definizione di "formato dei dati di tipo aperto" originariamente presente all'art. 68, comma 3, è stata integrata con la definizione di "dati di tipo aperto", grazie alle modifiche del 2012 al Codice dell'amministrazioni digitale. Successivamente, con le citate novelle del 2017 sul Cad, anche la definizione di "dati di tipo aperto" è confluita nell' art. 1, comma 1, lett. l-*ter*).
20. Per una distinzione fra *open format* e *open data*, si rinvia a Macrì 2021.
21. Corte di giustizia dell'Unione europea, sez. X, 21 novembre 2024, causa C-336/23.

anche i programmi informatici nella definizione di documento, possibilità che il legislatore italiano ha deciso di non cogliere, stabilendo espressamente che la definizione di documento non comprende i programmi informatici (art. 2, comma 1, lett. c), d.lgs. n. 36/2006). Il d.lgs. n. 36/2006 non definisce il "dato" in sé, ma il "dato pubblico", come il dato conoscibile da chiunque (art. 2, comma 1, lett. d), d.lgs. n. 36/2006) e i "dati personali" rinviando al regolamento europeo in materia 2016/679 (art. 2, comma 1, lett. g), d.lgs. n. 36/2006).

Le linee guida Agid in materia di apertura dei dati[22] rilevano la mancata chiarezza nella distinzione tra "documento" e "dato", osservando, al riguardo, che la normativa europea fa coincidere la definizione di "dato" con quella di "documento". Le stesse linee guida Agid, però, tracciano una differenza fra il concetto di dato e documento basata sul supporto per la loro rappresentazione. Secondo le linee guida Agid, infatti, la distinzione è che nel caso di "dato" è considerata solo la sua rappresentazione digitale, mentre nel caso di "documento" è compresa anche la rappresentazione attraverso supporto cartaceo. Pur riconoscendo che i termini di dati e documenti nella disciplina europea sono utilizzati come sinonimi, e anzi che i dati dinamici, i dati della ricerca e le serie di dati di elevato valore sono definiti nella direttiva 2019/1024 proprio come "documenti", le linee guida Agid, tuttavia, stabiliscono che "i dati" e "le informazioni" sono da vedersi come il contenuto, mentre il "documento" rappresenta il loro contenitore, osservando, a conferma di tale tesi, che l'articolo 1, comma 1 del d.lgs. n. 36/2006 disciplina il riutilizzo di "documenti contenenti dati pubblici"[23]. A ben guardare, però, a partire dal 2021, con le modifiche prodotte al d.lgs. n. 36/2006 dal d.lgs. 8 novembre 2021, n. 200 di attuazione della direttiva 2019/1024, anche il legislatore italiano definisce i "dati" come "documenti" per i dati dinamici, i dati della ricerca e le serie di dati di elevato valore (art. 2, comma 1, lett. c-sexies), c-*septies*), c-*octies*), d.lgs. n. 36/2006 e art. 2, punti 8), 9) e 10) della direttiva 2019/1024). Con il recepimento della direttiva 2019/1024, quindi, il legislatore italiano traspone la visione europea di equivalenza fra "dati" e "documenti", azzerandone così le differenze messe in rilievo dalle linee guida Agid e, consentendo, d'ora in avanti, di utilizzare i termini di "dati" e "documenti" come sinonimi.

3.2. Nozione di dati aperti

La direttiva non individua esattamente cosa si intenda per apertura dei dati, ma precisa che il concetto di apertura dei dati si intende generalmente riferito a dati in formati aperti che possono essere utilizzati, riutilizzati e condivisi liberamente da chiunque e per qualsiasi finalità (considerando 16, direttiva 2019/1024). Il decreto di recepimento della direttiva, d.lgs. n. 36/2006, all'art. 2, comma 1, lett. c-*quater*), invece, fornisce una definizione precisa di dati aperti rinviando al Codice dell'amministrazione digitale, che, in modo ricorsivo, a sua volta, cita lo stesso d.lgs. n. 36/2006. Il Codice dell'amministrazione digitale stabilisce sostanzialmente che i dati sono di tipo aperto quando sono caratterizzati sotto il profilo legale, tecnico ed economico. Con riferimento al primo profilo, il Cad prevede che i dati di tipo aperto sono resi disponibili secondo i termini di una licenza o di una previsione normativa che ne permetta l'utilizzo da parte di chiunque, per qualsiasi finalità, comprese quelle commerciali, in formato disaggregato. Sotto il profilo tecnico il Cad richiede che i dati di tipo aperto siano accessibili in rete in modalità digitale, in formati aperti e cosiddetti *machine readable*, ossia adatti all'utilizzo automatico da parte di programmi per elaboratori. Per quanto attiene al profilo economico, i dati di tipo aperto sono caratterizzati dal fatto di essere gratuiti, fatta salva la possibilità di recuperare i costi marginali derivanti dalla loro riproduzione, messa a disposizione, anonimizzazione o comunque protezione delle informazioni riservate ivi contenute (art. 1, comma 1, lett. l-*ter*), d.lgs. n. 82/2005).

3.3. Dati aperti di qualità

La qualità, diversamente dagli aspetti tecnici, economici e legali sopra esposti, non è un elemento caratterizzante i dati aperti, pur costituendo una componente fondamentale per il loro riutilizzo. Se si eccettuano i dati geospaziali, per i quali la disciplina italiana ne affida all'Istituto Geografico

22. *Linee guida recanti regole tecniche per l'apertura dei dati e il riutilizzo dell'informazione del settore pubblico*, adottate dall'Agid con la determina n. 183 del 3 agosto 2023.

23. *Ivi*, pp. 27 e 28.

Militare la raccolta, produzione, aggiornamento, riproduzione e diffusione, in modo da garantirne la qualità (art. 12-*bis*, comma 2, d.lgs. n. 36/2006), la direttiva europea, come pure il decreto di recepimento, non impongono specifiche disposizioni in materia di qualità dei dati alle amministrazioni titolari. La direttiva, tuttavia, osserva che il riutilizzo dei dati non rappresenta soltanto un arricchimento per il riutilizzatore, ma, in molti casi, anche per l'amministrazione che mette a disposizione i propri dati. Se il processo di apertura dei dati, infatti, promuove la trasparenza e responsabilizza l'ente, i riscontri provenienti da chi riutilizza questi dati permettono all'ente di migliorare la qualità dei propri dati (considerando 14).

Per definire la qualità dei dati occorre fare riferimento allo standard internazionale ISO/IEC 25012:2008, recepito come standard italiano nel 2014 (UNI CEI ISO/IEC 25012:2014). Il suddetto standard individua quindici distinte caratteristiche suddivise in tre categorie:

- "inerenti" (accuratezza, aggiornamento (attualità), completezza, consistenza (coerenza), credibilità);
- "inerenti e dipendenti dal sistema" (accessibilità, comprensibilità, conformità, efficienza, precisione, riservatezza, tracciabilità);
- "dipendenti dal sistema" (disponibilità, portabilità e ripristinabilità).

Per quanto premesso, le linee guida Agid si limitano a "raccomandare" – senza definire un vero e proprio obbligo per le amministrazioni – di garantire, per tutti i dati, in generale, e per quelli resi disponibili per il riutilizzo, in particolare, il rispetto almeno delle prime quattro caratteristiche sopra elencate: accuratezza, coerenza, completezza e attualità. Resta inteso che alcune di queste caratteristiche sono già insite nel rispetto di altre norme; ad esempio, la riservatezza dei dati è prevista dal relativo Regolamento europeo 2016/679, l'accessibilità è prevista dalla legge n. 4/2004, cosiddetta legge Stanca. Le amministrazioni, quindi, nel pubblicare i loro dati aperti si concentreranno su:

- l'accuratezza (sintattica e semantica), che si ottiene quando il dato e i suoi attributi rappresentano correttamente il valore reale del concetto o dell'evento a cui si riferiscono;
- la coerenza, ossia la caratteristica per la quale il dato e i suoi attributi non presentano contraddittorietà rispetto ad altri dati del contesto d'uso dell'amministrazione che detiene il dato;
- la completezza, che, come intuibile, richiede che il dato risulti esaustivo, sia per tutti i suoi valori attesi e sia rispetto alle fonti che concorrono alla definizione del procedimento al quale si riferisce;
- l'attualità, o tempestività di aggiornamento, grazie alla quale il dato e i suoi attributi sono aggiornati rispetto al procedimento cui si riferiscono.

Mentre lo standard 25012 definisce la qualità del dato, per la sua valutazione è possibile fare riferimento allo standard UNI CEI ISO/IEC 25024:2016 "Misurazione della qualità del dato", che individua molteplici controlli per ciascuna caratteristica di qualità. Con riferimento a ciascuna delle quattro caratteristiche principali, le linee guida Agid riportano alcuni dei possibili controlli. Per misurare la coerenza dei dati, ad esempio, un possibile controllo consiste nell'identificare quante volte si verifichi una violazione di regole semantiche definite su alcuni elementi dei dati (ad esempio, se una persona ha "il diritto di voto" la sua età dovrà essere maggiore o uguale di "18 anni"). Un altro controllo per misurare la coerenza è verificare il numero di valori duplicati in una base dati rispetto al numero totale degli elementi della base dati.

Aumentare la qualità dei dati e dei metadati è uno degli obiettivi assegnati alle pubbliche amministrazioni, contenuti all'interno del Piano triennale per l'informatica nella pubblica amministrazione. Con specifico riferimento alla qualità dei dati, il Piano triennale richiede un aumento del numero di dataset con metadati di qualità conformi agli standard di riferimento europei e nazionali, oltre che l'aumento del numero di dataset documentati sul portale dati.gov.it che rispettano la caratteristica di qualità "attualità" (o tempestività di aggiornamento) di cui allo standard ISO/IEC 25012:2008[24]. Se, quindi, il decreto sull'apertura dei dati e il riutilizzo dell'informazione pubblica non prevede l'obbligo per le amministrazioni di produrre dati aperti coerenti con i princìpi di qualità sopra illustrati, di fatto le Amministrazioni sono,

24. Piano triennale per l'informatica nella pubblica amministrazione, edizione 2024-2026, aggiornamento 2026, p. 143, RA5.2.4.

in ogni caso, invitate a procedere in tale senso in attuazione di quanto previsto dal richiamato Piano triennale. Sulla qualità del dato, d'altra parte, si giocherà la partita dell'intelligenza artificiale: la qualità delle risposte che i sistemi di intelligenza artificiale potranno fornire è strettamente correlata alla qualità dell'informazione che avranno a disposizione come input per funzionare.

4. Ambito di applicazione

Molto articolato è l'ambito di applicazione della normativa in materia di apertura dei dati e riutilizzo dell'informazione, che è possibile suddividere in due macro-insiemi: da un lato i soggetti che producono i documenti, dall'altro lato i documenti ai quali la disciplina si riferisce.

4.1. Soggetti produttori di dati

I soggetti tenuti a consentire il riutilizzo dei loro documenti, secondo l'art. 1 del d.lgs. n. 36/2006, sono sia pubbliche amministrazioni sia determinate imprese pubbliche o che svolgono servizi di pubblico interesse. In particolare, per pubbliche amministrazioni si intendono quelle del d.lgs. n. 165/2001[25], alle quali si aggiungono anche le autorità del sistema portuale, le autorità amministrative indipendenti di garanzia, vigilanza e regolazione, nonché i loro consorzi o associazioni (art. 2, comma 1, lett. a), d.lgs. n. 36/2006). Con specifico riferimento alle pubbliche amministrazioni, l'ambito di applicazione delineato dal decreto di recepimento della direttiva 2019/1024, se si eccettuano i consorzi e le associazioni delle pubbliche amministrazioni sopra indicate, è sovrapponibile con quello individuato dal Cad (art. 2, comma 2, lett. a), d.lgs. n. 82/2005). Al riguardo, però, occorre precisare che, mentre per il Cad sono espressamente escluse determinate amministrazioni quando si occupano di specifiche attività o svolgono determinate funzioni, ciò non vale per la disciplina sul riutilizzo. Il Cad opera, infatti, un'esclusione "limitatamente all'esercizio delle attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, polizia giudiziaria e polizia economico-finanziaria e consultazioni elettorali, nonché alle comunicazioni di emergenza e di allerta in ambito di protezione civile" (art. 2, comma 6, Cad). La disciplina in materia di riutilizzo, viceversa, non esclude *tout court* i soggetti preposti alla sicurezza nazionale. Il d.lgs. n. 36/2006, infatti, stabilisce che gli organismi preposti alla sicurezza nazionale, in particolare il Dipartimento delle informazioni per la sicurezza, l'Agenzia informazioni e sicurezza esterna, l'Agenzia informazioni e sicurezza interna, stabiliscono termini e modalità di riutilizzo secondo i rispettivi ordinamenti (art. 5, comma 6) e le linee guida Agid ribadiscono la medesima indicazione[26]. Dal che è possibile dedurre che – ferma restando l'esclusione di riutilizzo di dati segreti, come è logico aspettarsi – quando le succitate istituzioni producono dati pubblici e, in quanto tali, non soggetti al segreto, anche esse sono tenute a consentirne il riutilizzo, seppure nei termini e nelle modalità che esse stesse definiscono in autonomia. Tale interpretazione della soprarichiamata disposizione dell'art. 5, comma 6 del d.lgs. n. 36/2006 appare, tuttavia, in contrasto con quella contenuta nell'art. 3 dello stesso decreto, che, nell'elencare i documenti esclusi dalla sua applicazione, cita espressamente "quelli comunque nella disponibilità degli organismi di cui alla legge 3 agosto 2007, n. 124". Indipendentemente, quindi, dai tipi di documenti detenuti dagli organismi preposti al sistema di informazione per la sicurezza della Repubblica, quindi a prescindere dal fatto che trattasi di documenti classificati o meno, in ogni caso tali documenti non possono essere oggetto di riutilizzo (art. 3, comma 1, lett. e),

25. Per amministrazioni pubbliche si intendono 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'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN) e le Agenzie di cui al decreto legislativo 30 luglio 1999, n. 300, cosiddette Agenzie fiscali, oltre che il CONI (art. 1, comma 2, d.lgs. n. 165/2001).

26. *Linee guida recanti regole tecniche per l'apertura dei dati e il riutilizzo dell'informazione del settore pubblico*, cit., p. 77.

d.lgs. n. 36/2006). L'attuale formulazione di entrambe le disposizioni in commento del d.lgs. n. 36/2006 – art. 5, comma 6 e art. 3, comma 1, lett. e) – che risultano fra loro contrastanti è stata effettuata nel 2021 attraverso lo stesso d.lgs. n. 200/2021 di novella della disciplina per l'attuazione della direttiva 2019/2024. Al riguardo la relazione illustrativa relativamente alle modifiche dell'art. 3, comma 1, lett. e) parla di "modifica di mero coordinamento, atteso che la legge 24 ottobre 1977, n. 801, è stata abrogata dall'articolo 44 della legge 3 agosto 2007, n. 124", mentre con riguardo alle modifiche operate sull'art. 5 che stabilisce le modalità per la richiesta di riutilizzo, la novella intende fornire una "deroga" a tali modalità per una serie di soggetti. Nell'elencare tali soggetti il legislatore comprende anche quelli preposti alla sicurezza della Repubblica, che la norma, da sempre, escludeva dall'ambito di applicazione.

In aggiunta alle pubbliche amministrazioni, la disciplina in materia di apertura dei dati e riutilizzo dell'informazione si applica, altresì, alle imprese pubbliche e agli organismi di diritto pubblico[27], nonché, per taluni dati, alle imprese private soggette ad obblighi di servizio pubblico.

Mentre per le pubbliche amministrazioni e gli organismi di diritto pubblico nella definizione dell'ambito di applicazione non vi è alcun limite sull'attività svolta dall'istituzione, viceversa per le imprese, pubbliche e private, il provvedimento si applica solo quando l'impresa rientra in uno specifico settore di attività. In particolare, si stabilisce che le imprese pubbliche sono tenute a consentire il riutilizzo delle informazioni a loro disposizione qualora siano attive in settori quali, ad esempio, energia (gas, comprese le attività per la relativa estrazione, elettricità, ecc.), acqua, servizi di trasporto, porti e aeroporti, servizi postali[28], oppure come operatori di servizi pubblici di trasporto, compresi vettori aerei ed armatori comunitari che assolvono agli oneri di servizio pubblico (art. 1, comma 2-*ter*, d.lgs. n. 36/2006). Qualora l'impresa che presta il servizio di trasporto sia privata, ma svolge l'attività soggetta agli obblighi di servizio pubblico, sarà tenuta a consentire il riutilizzo dei propri dati (art. 1, comma 2-*quater*, d.lgs. n. 36/2006).

La novella al d.lgs. n. 36/2006 attuativa della direttiva 2019/1024 produce un considerevole ampliamento dell'ambito di applicazione, perché include le imprese pubbliche che la versione precedente escludeva espressamente. Come osservato dalla relazione illustrativa al decreto di recepimento della nuova direttiva in materia, d.lgs. 8 novembre 2021, n. 200, la nuova previsione è in linea con il considerando 19 della direttiva, che incoraggia gli Stati membri ad andare al di là dei requisiti minimi invitandoli ad applicare le disposizioni in materia di apertura dei dati e riutilizzo dell'informazione anche ai documenti detenuti da imprese pubbliche che operano su attività esposte alla concorrenza. Lo stesso considerando lascia la possibilità agli Stati membri di estendere la disciplina anche alle imprese private, in particolare quelle che forniscono servizi di interesse generale, possibilità della quale si è avvalsa l'Italia allargando conseguentemente l'ambito di applicazione del d.lgs. n. 36/2006.

Si tratta di un'importante sfida che coinvolge gli operatori del settore privato che risultano gestori di servizi pubblici, poiché sono chiamati a partecipare con la produzione dei loro dati all'attuazione della direttiva in materia di *open data* e riutilizzo, adeguandosi alla normativa sulla digitalizzazione, compresa quella regolamentare di Agid.

4.2. Dati oggetto di riutilizzo

I documenti detenuti da pubbliche amministrazioni, organismi di diritto pubblico e imprese pubbliche o private – come stabilito dall'art. 1, comma 1 del d.lgs. n. 36/2006 – sono oggetto di riutilizzo se contengono dati pubblici. Se, però, il documento, benché prodotto dalla pubblica amministrazione, non contiene dati pubblici, non ne può essere richiesto il riutilizzo in attuazione del d.lgs. n. 36/2006, poiché non rientra nell'ambito di applicazione, anche se allo stesso documento si applica la disciplina in materia di accesso (art. 3, comma 1, lett. h-*bis*), d.lgs. n. 36/2006). Quindi condizione necessaria al riutilizzo di un documento della pubblica amministrazione è che lo stesso contenga al suo interno

27. Per la definizione di organismi di diritto pubblico e imprese pubbliche, in particolare, l'art. 2, comma 1, lett. a-*bis*) e b) rinvia al d.lgs. 18 aprile 2016, n. 50, che disciplinava il codice dei contratti, ora trasfuso nel d.lgs. n. 36/2023.
28. Tali settori sono esplicitati dagli artt. da 115 a 121 del d.lgs. n. 50/2016 espressamente richiamato dall'art. 1, comma 2-*ter*, lett. a) del d.lgs. n. 36/2006.

dati pubblici, ossia dati conoscibili da chiunque. Sotto questo profilo, il raggio di azione della disciplina in materia di riutilizzo dell'informazione pubblica è ben delimitato dalla direttiva europea e dal decreto di recepimento italiano, anche se, come sopra accennato, il Regolamento relativo alla governance europea dei dati mira ad estendere la disciplina sul riutilizzo anche ai dati che non sono pubblici.

Dal 2021 la nuova versione dell'art. 1, comma 2 del d.lgs. n. 36/2006 amplia l'ambito di applicazione della disciplina in materia di riutilizzo, comprendendovi anche quei documenti sui quali biblioteche, musei ed archivi detengono i diritti di proprietà intellettuale, a meno che su tali documenti non vi siano dei limiti derivanti dalla normativa in materia di tutela dei dati personali (d.lgs. n. 196/2003) o dei beni culturali (d.lgs. n. 42/2004). Con specifico riferimento alla tutela dei dati personali, però, occorre chiarire che, come immaginabile, nell'art. 3, che ha per rubrica "Documenti esclusi dall'applicazione del decreto" il d.lgs. n. 36/2006 ribadisce l'esclusione di applicazione della disciplina in materia di riutilizzo per quei documenti il cui accesso risulti pregiudizievole per la tutela della vita privata e dell'integrità degli individui (comma 1, lett. h-*quater*). Con ciò è possibile, quindi, dedurre che, se un documento pone dei limiti di privacy, esso non potrà essere oggetto di riutilizzo, in quanto non si tratta di un dato aperto. In tal senso, quindi, la disciplina sul riutilizzo delineata dal d.lgs. n. 36/2006, nella definizione del suo ambito di applicazione prende in considerazione quei dati pubblici, ossia conoscibili da chiunque, che non pongono esigenza di tutela della privacy.

Le novelle del 2021 estendono la disciplina sul riutilizzo anche ai dati sulla ricerca (art. 1, comma 2-*bis* e articolo 9-*bis*, d.lgs. n. 36/2006), dati che, viceversa, la precedente versione del decreto espressamente escludeva dal riutilizzo. Con specifico riferimento ai dati della ricerca risultanti da progetti finanziati attraverso fondi pubblici, l'art. 1, comma 2-*bis* del d.lgs. n. 36/2006 ne stabilisce il riutilizzo, che però non è incondizionato, ma – ancora una volta si precisa – limitato dalla disciplina in materia di tutela della privacy, oltre che da quella in materia di proprietà intellettuale (d.lgs. n. 633/1941) e di proprietà industriale (d.lgs. n. 30/2005). Se, però, gli istituti di ricerca producono dati che non rientrano esattamente nella definizione di dati della ricerca, allora per questi non vige l'obbligo del riutilizzo (art. 3, comma 1, lett. h-sexies), d.lgs. n. 36/2006).

Fra i dati oggetto di riutilizzo, però, ve ne sono alcuni che emergono in rilievo rispetto agli altri, perché, come significativamente indicati dalla norma, si tratta di dati di elevato valore, per i quali lo stesso legislatore europeo, al fine di armonizzarne il trattamento fra tutti gli Stati membri, è intervento con un Regolamento di esecuzione.

Il dato prodotto da pubbliche amministrazioni e organismi di diritto pubblico può essere oggetto di riutilizzo se il soggetto produce o, comunque, detiene quel dato per finalità istituzionali. I dati che esulano dai compiti istituzionali, infatti, sono espressamente sottratti dalla disciplina in materia di riutilizzo (art. 3, comma 1, lett. a), d.lgs. n. 36/2006). Analogamente non rientrano nell'ambito di applicazione del d.lgs. n. 36/2006 quei dati che le imprese producono nell'ambito di prestazioni che non risultano di interesse generale, oppure sono dati connessi ad attività esposte alla concorrenza e non soggette alla disciplina in materia di appalti (art. 3, comma 1, lett. a-*bis*), d.lgs. n. 36/2006).

Il decreto, inoltre, esclude dal riutilizzo una serie di dati, individuati sulla base del soggetto titolare o delle loro caratteristiche. I dati, come già richiamato, prodotti da soggetti che si occupano della sicurezza nazionale (art. 3, comma 1, lett. e), d.lgs. n. 36/2006), oppure i dati prodotti da emittenti di servizio pubblico, quindi la Rai, o da loro controllate per la radiodiffusione non sono oggetto di riutilizzo (art. 3, comma 1, lett. b), d.lgs. n. 36/2006). Allo stesso tempo non sono oggetto di riutilizzo i dati di istituti scolastici o enti culturali che non siano biblioteche, musei e archivi (art. 3, comma 1, lett. c) e d) D.Lgs. n. 36/2006).

Come intuibile, il dato che è escluso dalla disciplina in materia di diritto di accesso (art. 24, legge 7 agosto 1990, n. 241), come ad esempio il dato coperto da segreto di Stato, o il dato sottratto alla disciplina in materia di accesso civico (art. 5-*bis*, d.lgs. 14 marzo 2013, n. 33), come ad esempio il dato relativo alle relazioni internazionali, alla politica e alla stabilità economica e finanziaria dello Stato, o il dato relativo alle informazioni sensibili sulle infrastrutture critiche del Paese, neppure è esigibile ai fini del riutilizzo (art. 3, comma 1,

lett. h-*quinquies*), d.lgs. n. 36/2006[29]). Anche il dato statistico è escluso dalla disciplina in materia di riutilizzo, qualora ciò comporti una violazione del segreto statistico (art. 3, comma 1, lett. g), d.lgs. n. 36/2006) [30].

Se il documento contiene solo logotipi, stemmi e distintivi o se il documento è oggetto di diritti di proprietà intellettuale o industriale da parte di terzi, non potrà essere oggetto di riutilizzo (art. 3, comma 1, lett. h) ed h-*ter*, d.lgs. n. 36/2006).

L'art. 4 del d.lgs. n. 36/2006 (comma 1, lett. a), b), c), e) individua le discipline fatte salve dal riutilizzo: disciplina in materia di protezione dei dati personali, diritto di autore, accesso ai documenti amministrativi, proprietà intellettuale. La norma di salvaguardia relativa alla disciplina in materia di dati personali, frutto dell'interlocuzione con gli Uffici dell'Autorità garante per la protezione dei dati personali[31], peraltro, è ribadita anche a proposito dei dati della ricerca (art. 9-*bis*, d.lgs. n. 36/2006), inizialmente esclusi e poi inseriti con le novelle del 2021. Come già richiamato, oggetto di riutilizzo sono, fra l'altro, i dati che le amministrazioni devono pubblicare sulla sezione trasparenza, per alcuni dei quali potrebbe porsi l'esigenza di tutela dei dati personali. L'Anac, al riguardo, ha chiarito che gli obblighi di pubblicazione previsti dal d.lgs. 33/2013 sono compatibili con la disciplina della tutela dei dati personali dettata dal Regolamento (UE) 2016/679 (RGPD), in quanto "l'art. 2-*ter* del d.lgs. n. 196/2003, introdotto a seguito dell'entrata in vigore del Regolamento (UE) 2016/679, dispone che la base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, ai sensi del Regolamento (UE) 2016/679 'è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento' (art. 6, paragrafo 3, lett. b). Ne discende che, essendo gli obblighi di pubblicazioni del d.lgs. 33/2013 previsti da un decreto legislativo, sono pienamente compatibili con la nuova disciplina in materia di protezione dei dati personali"[32]. Da questo chiarimento dell'Anac è possibile dedurre che i dati rientranti nell'ambito di applicazione della disciplina in materia di riutilizzo quando contengono dati personali, ma sono comunque sottoposti agli obblighi di pubblicazione del d.lgs. 33/2013, sono anch'essi *pienamente compatibili con la nuova disciplina in materia di protezione dei dati personali*. In altri termini, i dati che possono essere pubblicati per la disciplina sulla trasparenza, potranno anche essere riutilizzati, a meno che non vi sia un limite temporale alla loro pubblicazione.

Fermo restando le limitazioni sopra richiamate al diritto di riutilizzo, pubbliche amministrazioni o organismi di diritto pubblico non potranno far valere alcun altro diritto per limitare o negare il riutilizzo di documenti contenenti dati pubblici. Al proposito, infatti, l'art. 3 del d.lgs. n. 36/2006 esplicita che le pubbliche amministrazioni non possono avvalersi del diritto esclusivo di riproduzione e distribuzione parziale o integrale di una banca dati della quale sono titolari, diritto sancito dall'art. 64-*quinquies* della legge 22 aprile 1941,

29. La norma rinvia all'art. 2, d.lgs. n. 61/2011, abrogato, a partire dal 18 ottobre 2024, dal più recente d.lgs. n. 134/2024 che recepisce la nuova direttiva, cosiddetta NIS2, in materia di resilienza dei soggetti critici.
30. Nella prima versione del 2006 del decreto di recepimento della previgente direttiva 2003/98 era stata prevista fra le norme di salvaguardia la disciplina sul sistema statistico nazionale. Con le novelle del 2010, operate dalla legge comunitaria del 2009 (legge 4 giugno 2010, n. 96), sono state abrogate le disposizioni che includevano fra le norme di salvaguardia i dati catastali e i dati statistici (art. 4, lett. d) ed f), d.lgs. n. 36/2006). Con riferimento ai dati statistici, però, resta salvaguardato il segreto statistico, come espressamente indicato dall'art. 3, comma 1, lett. g) del d.lgs. n. 36/2006. Ciò implica che i dati raccolti nell'ambito di rilevazioni statistiche comprese nel programma statistico nazionale da parte degli uffici di statistica non possono essere esternati se non in forma aggregata e possono essere utilizzati solo per scopi statistici (art. 9, comma 1, d.lgs. n. 322/1989, che disciplina la tutela del segreto statistico).
31. Garante per la protezione dei dati personali, Parere sullo schema di decreto legislativo recante "Attuazione della Direttiva (UE) 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico", registro dei provvedimenti n. 308 del 26 agosto 2021.
32. Anac, FAQ in materia di trasparenza (sull'applicazione del d.lgs. n. 33/2013 come modificato dal d.lgs. 97/2016), aggiornate al 30 luglio 2020, punto 7.1.

n. 633, per impedire o limitare il riutilizzo di loro documenti. In altri termini, qualsiasi soggetto rientrante nell'ambito di applicazione della disciplina sul riutilizzo che gestisce una banca dati dovrà consentire il riutilizzo delle informazioni ivi contenute non potendo impedirlo in forza della normativa del 1941 in materia di diritto d'autore, così come modificata negli anni Novanta in attuazione della cosiddetta direttiva database (dir. 96/9/CE).

5. Procedure per il riutilizzo delle informazioni e forme di tutela

L'art. 5 del d.lgs. n. 36/2006 specifica, per le amministrazioni e gli organismi di diritto pubblico, le procedure da seguire quando viene formulata una richiesta per il riutilizzo dei dati e, per i soggetti interessati al riutilizzo, le forme di tutela attivabili.

Le istituzioni pubbliche, ossia pubbliche amministrazioni o organismi di diritto pubblico, hanno trenta giorni di tempo decorrenti dalla richiesta del soggetto interessato al riutilizzo per esaminare le richieste e rendere disponibili i documenti. Se l'amministrazione è in affanno per la numerosità o la complessità delle richieste, entro il ventunesimo giorno dalla richiesta, è tenuta a informare il richiedente che la risposta verrà fornita, anziché entro i trenta giorni stabiliti in condizioni standard, entro cinquanta giorni (art. 5, comma 1, d.lgs. n. 36/2006). Dall'applicazione dell'articolo 5 sono escluse le imprese, gli istituti di istruzione e di ricerca, oltre che le istituzioni che si occupano di sicurezza nazionale, perché definiscono le modalità per il riutilizzo secondo i propri ordinamenti (art. 5, comma 6). Sembra, quindi, che il d.lgs. n. 36/2006 intenda individuare due regimi distinti a seconda delle pubbliche amministrazioni interessate. Da un lato, la generalità delle amministrazioni, alle quali si applica la disciplina sul riutilizzo, che ha, complessivamente, fino a un massimo di cinquanta giorni di tempo, dall'altro lato, imprese, istituti di istruzione e di ricerca, istituzioni che si occupano di sicurezza nazionale, che, in linea teorica, potrebbero dilatare *ad libitum*, l'arco temporale per evadere la richiesta di riutilizzo dei loro documenti. Al riguardo, però, le linee guida Agid cercano di porre un argine, ribadendo che, pur nella loro autonomia organizzativa, i soggetti sopra elencati dovranno in ogni caso rispettare i termini definiti dal decreto, che prevede un termine massimo di trenta giorni dalla data della richiesta, prorogabile di ulteriori 20 giorni, per ottemperare al rilascio dell'informazione pubblica da riutilizzare[33].

Quando la richiesta viene accolta, l'istituzione fornisce i documenti richiesti per il riutilizzo "ove possibile, in forma elettronica" e "se necessario" attraverso una licenza d'uso (art. 5, comma 2, d.lgs. n. 36/2006). L'espressione "ove possibile, in forma elettronica" è utilizzata dal legislatore già nella prima versione del 2006 del decreto in materia di riutilizzo dell'informazione pubblica. L'obiettivo era evidentemente quello di precisare che le istituzioni pubbliche non avrebbero dovuto sostenere ulteriori oneri per consentire il riutilizzo delle loro informazioni, laddove queste non fossero già state prodotte in formato elettronico. Tale disposizione era pienamente giustificabile se rapportata allo stato di maturazione della digitalizzazione della pubblica amministrazione italiana del momento. Nel gennaio 2006, infatti, il Cad, benché pubblicato in Gazzetta ufficiale il 7 marzo 2005, era appena entrato in vigore. Il differimento della sua vigenza era stato valutato necessario: si voleva offrire alle pubbliche amministrazioni il tempo sufficiente per operare tutti gli adeguamenti tecnologici necessari a garantire il diritto all'uso delle tecnologie da parte dei cittadini e delle imprese nei rapporti con le pubbliche amministrazioni (art. 3, comma 1 della prima versione del Cad). Il decreto di novella del d.lgs. n. 36/2006, a distanza di 15 anni dalla prima versione, non espunge l'inciso "ove possibile", ma si attiene alla direttiva 2019/1024, che anch'essa stabilisce che gli enti pubblici e le imprese pubbliche mettono a disposizione i propri documenti in qualsiasi formato o lingua preesistente e, "ove possibile e opportuno", per via elettronica (art. 5, par. 1). Allorquando si definiscono le modalità tecniche con le quali amministrazioni pubbliche, organismi di diritto pubblico e imprese pubbliche, nonché le imprese private del settore dei trasporti, mettono a disposizione i propri documenti, si rinvia – *inequivocabilmente* – alla modalità digitale. Se ne esplicitano, infatti, i formati, che devono essere *machine readable*, cioè leggibili in automatico da programmi software *ad hoc*, e di tipo aperto

33. *Linee guida recanti regole tecniche per l'apertura dei dati e il riutilizzo dell'informazione del settore pubblico*, cit., p. 77.

e si stabilisce, in ogni caso, che i documenti devono essere prodotti secondo le linee guida Agid in materia di formati aperti (art. 6, comma 1 e comma 7, d.lgs. n. 36/2006). Se letto alla luce del nuovo Regolamento eIDAS, che stabilisce l'equivalenza del documento elettronico con quello cartaceo[34], e del principio *digital first* – in conseguenza del quale se un'amministrazione per lo svolgimento di un'attività istituzionale può utilizzare sia la modalità tradizionale, sia quella digitale, deve preferire quest'ultima – l'espressione "ove possibile" appare oggi superata. La sua applicazione letterale, quindi, sarebbe da limitarsi a documenti datati, originariamente prodotti in modalità cartacea e per i quali l'amministrazione non abbia ritenuto conveniente una loro digitalizzazione. A conferma di tale interpretazione, le pubbliche amministrazioni, oltre che gli organismi di diritto pubblico, le imprese pubbliche e private del settore dei trasporti, quando si trovano a produrre documenti che rientrano nell'ambito di applicazione della disciplina in materia di riutilizzo, devono produrli secondo il principio cosiddetto dell'*open by default* (art. 6, commi 4 e 7, d.lgs. n. 36/2006). Ciò significa che già nella fase di progettazione il dato, quando viene prodotto o raccolto, deve essere conforme alle regole tecniche in materia di apertura dei dati; il dato pubblico, quindi, deve nascere digitale. Per quanto attiene ai dati e documenti già prodotti, invece, si stabilisce che le amministrazioni, gli organismi di diritto pubblico, le imprese pubbliche e private del settore dei trasporti non sono tenute ad adeguare i loro documenti, o parti di essi, per consentirne il riutilizzo se ciò comporta difficoltà sproporzionate (art. 6, commi 2 e 7, d.lgs. n. 36/2006). Nell'ipotesi che la richiesta formulata per il riutilizzo non venisse accolta, allora amministrazioni, organismi di diritto pubblico, imprese pubbliche e private del settore dei trasporti dovranno motivare il rifiuto (art. 5, comma 3 e art. 6, commi 2 e 7, d.lgs. n. 36/2006). Nel caso che il diniego sia dovuto a diritti di proprietà intellettuale o industriale, l'amministrazione pubblica o l'organismo di diritto pubblico dovrà indicare all'interessato le informazioni necessarie per ottenere il materiale, come ad esempio la persona fisica o giuridica titolare del dato. Biblioteche, archivi e musei dovranno semplicemente motivare il diniego, senza preoccuparsi di fornire ulteriori elementi (art. 5, commi 3 e 4, d.lgs. n. 36/2006).

Le linee guida Agid[35] definiscono indicazioni pratiche per la richiesta di riutilizzo, stabilendo che essa – a meno che l'amministrazione non abbia individuato già attraverso un proprio ordinamento la procedura per l'accesso ai propri dati ai fini del riutilizzo – può essere rivolta ad uno degli uffici indicati dalla disciplina in materia di accesso civico: all'ufficio che detiene i dati, le informazioni o i documenti; all'ufficio relazioni con il pubblico; ad altro ufficio indicato dall'amministrazione nella sezione "Amministrazione trasparente" del sito istituzionale; al responsabile della prevenzione della corruzione e della trasparenza, ove l'istanza abbia ad oggetto dati, informazioni o documenti oggetto di pubblicazione obbligatoria in attuazione del d.lgs. 33/2013. Le indicazioni che emergono dalle linee guida, pertanto, sono nell'ottica di conformare le procedure per il riutilizzo a quelle per l'accesso civico. Qualora, però, la pubblica amministrazione o l'organismo di diritto pubblico neghino il riutilizzo, le tutele del cittadino o dell'impresa che hanno bisogno di riutilizzare l'informazione pubblica non sono quelle proprie dell'accesso civico. L'art. 5, comma 5 del d.lgs. n. 36/2006, infatti, stabilisce che gli strumenti a tutela del soggetto interessato al riutilizzo dell'informazione pubblica sono gli stessi previsti dalla legge in materia di diritto di accesso (legge 7 agosto 1990, n. 241, articolo 25, commi 4 e 5) e non già in materia di accesso civico (d.lgs. n. 33/2013). Quindi se il titolare di dati ne negasse il riutilizzo, il soggetto interessato potrà adire il giudice amministrativo, oppure il difensore civico competente territorialmente o la Commissione per l'accesso (anche se ulteriori strumenti di tutela potrebbero essere utilizzati, come meglio evidenziato nel par. 5.2). A partire

34. "*A un documento elettronico non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica*", art. 46, Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

35. *Linee guida recanti regole tecniche per l'apertura dei dati e il riutilizzo dell'informazione del settore pubblico*, cit., p. 76 ss.

dalla data di entrata in vigore del d.lgs. n. 36/2006 novellato con le disposizioni sopra richiamate, tuttavia, non risulta alcuna pronuncia in materia di riutilizzo dell'informazione pubblica fra quelle pubblicate dalla Commissione per l'accesso. Viceversa, in molteplici sue pronunce la Commissione per l'accesso ribadisce la propria incompetenza nel decidere sulla presunta disapplicazione del d.lgs. n. 33/2013[36]. Ci si chiede, quindi, se la scelta del legislatore italiano di tutelare la materia sul riutilizzo dell'informazione pubblica attraverso strumenti propri del diritto di accesso (legge n. 241/1990) sia quella più coerente, anche in considerazione della sopracitata sentenza della Corte di giustizia dell'Unione europea, secondo la quale il riutilizzo e l'accesso ai documenti rappresentano "due operazioni manifestamente distinte". Il Consiglio di Stato, peraltro, ha segnato un'ulteriore distinzione fra il diritto al riutilizzo e il diritto all'accesso, stabilendo che il silenzio dell'amministrazione alla richiesta al riutilizzo non può essere trattato alla stessa stregua del silenzio dell'amministrazione in caso di richiesta di accesso. A seguito della richiesta di riutilizzo, infatti, occorre che vi sia necessariamente un provvedimento di accoglimento o di rigetto, in tale ultimo caso motivato, in quanto l'inerzia dell'amministrazione non equivale al rigetto. Nel caso di richiesta di accesso, invece, il silenzio dell'amministrazione, decorsi i termini, è da intendersi quale rigetto. Si legge nella citata sentenza che il "tenore letterale della norma" – contenuta nell'art. 5, comma 5, d.lgs. n. 36 del 2006 – "secondo la quale: 'In caso di diniego, il richiedente può esperire i mezzi di tutela previsti dall'articolo 25, commi 4 e 5, della legge 7 agosto 1990, n. 241. Degli stessi è data comunicazione al richiedente con il provvedimento di diniego' induce a ritenere che il legislatore abbia inteso estendere al caso di diniego di autorizzazione al riutilizzo dei documenti pubblici gli stessi rimedi, amministrativi e giurisdizionali, previsti per il caso di diniego di accesso agli atti. Tale equiparazione, non riguarda, però, la formazione del silenzio rigetto, prevista, in materia di accesso agli atti, dall'art. 24, comma 4, primo periodo, legge n. 241 del 1990, con la conseguenza che, in materia di autorizzazione al riutilizzo, rimane comunque necessaria l'adozione di un provvedimento espresso da parte della competente Amministrazione"[37].

5.1. Riutilizzo di dati in esclusiva

Qualora i dati siano stati forniti, una prima volta, per il loro riutilizzo, in ogni caso restano comunque sottoposti alla disciplina in materia di riutilizzo, perché fra i princìpi sanciti dal decreto in materia vi è quello relativo alla parità di trattamento fra i soggetti interessati al riutilizzo, fermo restando la possibilità di accordi di esclusiva. Il d.lgs. n. 36/2006 stabilisce, come sopra richiamato, che, quando il soggetto mette a disposizione i suoi dati definendone le condizioni per il riutilizzo, ad esempio attraverso una licenza d'uso, deve aver cura che tali condizioni non comportino discriminazioni per categorie analoghe di riutilizzo, compreso il riutilizzo transfrontaliero, né costituiscano ostacolo alla concorrenza (art. 8, comma 4). Ciò significa che, se Tizio chiede il riutilizzo di un determinato set di dati e, in un momento successivo, arriva Caio, benché di altro Stato membro, che, ad esempio, per lo sviluppo della propria attività imprenditoriale ha bisogno di riutilizzare lo stesso set di dati, il soggetto che di quei dati è titolare sarà tenuto a consentirne il riutilizzo in applicazione del principio di non discriminazione, a meno che Tizio non abbia preventivamente instaurato con il titolare dei dati un accordo di esclusiva. In altri termini un dato già riutilizzato non per questo non potrà nuovamente essere riutilizzato, a meno che su di esso non vi sia un accordo di esclusiva. Dal principio di parità di trattamento e non discriminazione, sancito dall'art. 1, comma 3 del d.lgs. n. 36/2006, discende che non è possibile prevedere diritti esclusivi nei contratti o comunque negli accordi che i titolari dei dati stipulano con i soggetti interessati al riutilizzo. Quindi i documenti delle pubbliche amministrazioni, come pure degli organismi di diritto pubblico e dei privati possono essere riutilizzati da chiunque, anche se già altri soggetti stiano sfruttando tali documenti (art. 11, comma 1, d.lgs. n. 36/2006). La disciplina

36. Da ultimo, seduta del 15 dicembre 2022 sul ricorso contro il Ministero dell'interno, Dipartimento di pubblica sicurezza, la Commissione per l'accesso ha osservato "di non essere competente a esaminare ricorsi relativi alle richieste di accesso civico generalizzato".

37. Cons. Stato, sentenza n. 2818/2025 pubblicata il 2 aprile 2025.

sul riutilizzo dell'informazione, pertanto, esclude, in linea generale, accordi che prevedano la possibilità di riutilizzo di dati o documenti in esclusiva. Tuttavia, come evidenziato nel considerando 49 della direttiva 2019/1024, negli Stati membri vi sono numerosi accordi di cooperazione tra biblioteche, musei, archivi e soggetti privati che prevedono la digitalizzazione di risorse culturali con diritti di esclusiva a soggetti privati. Ciò in quanto il soggetto privato ha bisogno di un certo periodo di esclusiva per poter recuperare il proprio investimento. Per tenere conto di tali situazioni, oltre che delle differenze tra gli Stati membri in materia di digitalizzazione delle risorse culturali, la direttiva si è posta l'obiettivo di individuare il periodo più breve possibile per rispettare il principio secondo cui i materiali di dominio pubblico dovrebbero rimanere tali una volta digitalizzati, indicando un periodo massimo per l'esclusiva non superiore a dieci anni e prevedendo un articolato scadenzario (art. 12, dir. 2019/1024). Il legislatore italiano, nel recepire la direttiva, riduce questo periodo a sette anni e stabilisce, analogamente alla tariffazione, un regime distinto per la "digitalizzazione di risorse culturali" da un lato e per quelle delle pubbliche amministrazioni, degli organismi di diritto pubblico e delle imprese pubbliche dall'altro. Con riferimento a questi ultimi si stabilisce che, qualora per l'erogazione di un servizio di interesse pubblico sia necessario un diritto esclusivo sui dati, ogni tre anni occorre valutare le motivazioni con le quali è stato attribuito tale diritto esclusivo. In ogni caso il soggetto titolare dei dati, almeno due mesi prima che abbiano effetto tali accordi di esclusiva, procede alla loro pubblicazione sul proprio sito istituzionale (art. 11, comma 2, d.lgs. n. 36/2006). L'indicazione relativa alla pubblicità è, altresì, ribadita dal successivo comma 4 dell'art. 11, d.lgs. n. 36/2006, che stabilisce, più in generale, che una qualsiasi disposizione che limiti la disponibilità di riutilizzo di dati, ancorché non si tratti di un vero e proprio diritto esclusivo, va resa pubblica almeno due mesi prima della sua efficacia e valutata periodicamente ogni tre anni. Se invece si tratta della digitalizzazione di risorse culturali, il periodo di esclusiva, di norma, non può superare i sette anni. L'ottavo anno si procede a un riesame e, se vi sono le condizioni, si rivaluta successivamente ogni cinque anni. Anche nel caso delle risorse culturali gli accordi di esclusiva sono soggetti a pubblicazione per motivi di trasparenza (art. 11, comma 3, d.lgs. n. 36/2006). Sono, inoltre, state previste delle specifiche disposizioni per disciplinare i diritti di esclusiva preesistenti al decreto di novella del d.lgs. n. 36/2006, in coerenza con la *ratio* della direttiva[38].

5.2. Obblighi di transizione digitale nel riutilizzo dell'informazione pubblica

Le modalità tecniche per il riutilizzo dei dati pubblici previste dalla disciplina antecedente al recepimento della direttiva 2019/1024 rinviavano al d.lgs. n. 42/2005 sul sistema pubblico di connettività, ben presto abrogato per confluire nel Codice dell'amministrazione digitale. Il sistema pubblico di connettività, però, non avrebbe mai potuto costituire il vero strumento con il quale realizzare da parte di un soggetto privato il riutilizzo di dati, non tanto per motivi tecnici, quanto per il semplice fatto che tale sistema era stato concepito come evoluzione del precedente modello di rete unitaria delle pubbliche amministrazioni, caratterizzata dall'essere aperta esclusivamente alle pubbliche amministrazioni. Con la conseguenza, quindi, che un privato non avrebbe potuto accedervi. Le successive modifiche intervenute sul decreto in materia di riutilizzo, però, non hanno mai offerto un vero e proprio strumento tecnico in mano ai soggetti privati interessati a esercitare il loro diritto al riutilizzo dei dati aperti fino all'entrata in vigore del d.lgs. n. 200/2021 di modifica del d.lgs. n. 36/2006. Con le novelle al d.lgs. n. 36/2006, fra l'altro, si precisano e definiscono i termini di adempimento,

38. Si stabilisce, in particolare, che i diritti di esclusiva concessi da pubbliche amministrazioni o da organismi di diritto pubblico preesistenti al 17 luglio 2013, che non sono conformi alle condizioni sopra richiamate per beneficiare di deroghe, vanno rivisti con cadenza almeno triennale per verificare la fondatezza del motivo di esclusiva e l'effetto di tali diritti cessa alla scadenza del contratto e comunque non oltre il 18 luglio 2043 (art. 11, comma 5). Nell'ipotesi che i diritti di esclusiva riguardino le imprese pubbliche, la revisione degli accordi è da effettuarsi con i medesimi obiettivi e nei medesi termini sopra richiamati e, in ogni caso, qualora gli accordi siano antecedenti al 16 luglio 2019, cessano alla scadenza del contratto e comunque non oltre il 16 luglio 2049 (art. 11, comma 6, d.lgs. n. 36/2006).

che nella precedente versione, ad esempio, mancavano di un termine *a quo*. Si stabiliva, al riguardo, che l'amministrazione provvedesse entro trenta giorni ad esaminare le richieste di riutilizzo dei documenti e a metterli a disposizione del richiedente, senza indicare il momento dal quale decorresse tale arco temporale. La previgente disciplina, inoltre, prevedeva che l'interessato dovesse presentare l'istanza per il riutilizzo secondo le modalità che indicava la singola amministrazione titolare del dato attraverso un proprio provvedimento. Ciò in quanto il Codice dell'amministrazione digitale, dopo la modifica operata dal Governo Monti con il d.l. 18 ottobre 2012, n. 179, convertito dalla legge 17 dicembre 2012, n. 221, prevedeva che le pubbliche amministrazioni pubblicassero nella sezione trasparenza del proprio sito web il catalogo dei dati, dei metadati e delle relative banche dati in loro possesso, oltre ai relativi regolamenti per l'accesso per fini istituzionali o di riutilizzo (art. 52, comma 1, del d.lgs. n. 82/2005, successivamente abrogato dall'art. 42, comma 1 del d.lgs. 26 agosto 2016, n. 179). Nei fatti però, tale disposizione trovò un'applicazione abbastanza limitata, anche in considerazione del fatto che un'eventuale inadempienza non avrebbe prodotto alcuna concreta conseguenza. Più esattamente, la mancata applicazione delle disposizioni del Cad produceva e produce una responsabilità disciplinare e dirigenziale, oltre che civile, penale e contabile per il soggetto incaricato (art. 12, comma 1-*ter*, d.lgs. n. 82/2005). Si tratta, tuttavia, di disposizioni che non hanno costituito un reale deterrente per l'applicazione della disciplina in materia di digitalizzazione delle pubbliche amministrazioni. A prova di tale considerazione, va osservato che a distanza di oltre dieci anni dalla data di entrata in vigore del Cad, la mancata digitalizzazione della pubblica amministrazione italiana ha costituito il tallone d'Achille del Paese, valutato dalle Istituzioni europee negli anni 2019 e 2020 come un freno alla nostra crescita economica[39].

Per dare piena attuazione alla nuova disciplina in materia di apertura dei dati e di riutilizzo dell'informazione pubblica, non solo si stabilisce che Agid deve mettere a disposizione delle linee guida, che sono state tempestivamente adottate, ma si stabilisce anche che, in caso di violazione delle disposizioni contenute nelle linee guida, il soggetto interessato può rivolgersi al difensore civico per il digitale e l'amministrazione, che non ha adempiuto alla normativa (secondaria) in materia di riutilizzo dell'informazione pubblica, può essere sottoposta a sanzioni (art. 12, d.lgs. n. 36/2006)[40].

In tal modo il legislatore sembrerebbe voler individuare due percorsi distinti per la tutela del diritto al riutilizzo dell'informazione pubblica: nel caso vi sia un'inadempienza rispetto alle disposizioni contenute nel d.lgs. n. 36/2006 le forme di tutela sono quelle previste per il diritto all'accesso, illustrate sopra nel par. 5; se viceversa l'inadempienza è con riguardo alle linee guida Agid in materia di apertura dei dati e riutilizzo, allora bisognerà rivolgersi al difensore civico per il digitale.

L'ufficio del difensore civico per il digitale è istituito presso l'Agid a garanzia dei diritti digitali di cittadini e imprese. Qualsiasi soggetto può presentare al difensore civico per il digitale, attraverso il sito istituzionale dell'Agid[41], segnalazioni relative a presunte violazioni di qualsiasi norma in materia di digitalizzazione ed innovazione della pubblica amministrazione, incluso, quindi, segnalazioni relative al mancato rispetto della disciplina sull'apertura dei dati e sul riutilizzo del settore pubblico.

39. Raccomandazione del Consiglio del 9 luglio 2019 sul programma nazionale di riforma 2019 dell'Italia e che formula un parere del Consiglio sul programma di stabilità 2019 dell'Italia (2019/C 301/12), GUUE C 301/69 del 5 settembre 2019; Raccomandazione del Consiglio del 20 luglio 2020 sul programma nazionale di riforma 2020 dell'Italia e che formula un parere del Consiglio sul programma di stabilità 2020 dell'Italia (2020/C 282/12), GUUE C 282/74 del 26 agosto 2020.

40. Tali sanzioni si applicano anche nel caso di dati territoriali, che rientrano nell'ambito del d.lgs. n. 32/2010, introdotto per il recepimento della direttiva 2007/2/CE, cosiddetta direttiva INSPIRE (acronimo di INfrastructure for SPatial InfoRmation in Europe), perché così espressamente deciso in sede di novella del d.lgs. n. 36/2006 (art. 1, comma 2-*quinquies*).

41. Da una specifica sezione del sito Agid è possibile segnalare al difensore civico il mancato rispetto del Codice dell'amministrazione digitale o di altre norme in materia di digitalizzazione e innovazione (esclusa la disciplina in materia di accessibilità per la quale si utilizzano altre modalità di segnalazione).

Il difensore civico per il digitale raccoglie le segnalazioni e, una volta che ne abbia accertata la non manifesta infondatezza, le trasmette al Direttore generale dell'Agid per l'esercizio dei poteri sanzionatori (art. 17, comma 1-*quater*, d.lgs. n. 82/2005).

Nel caso specifico Agid può applicare all'amministrazione inadempiente sanzioni che variano dai 10.000 euro ai 100.000 euro, come stabilito dall'art. 18-*bis*, comma 5 del Codice dell'amministrazione digitale. Tale disposizione disciplina le misure conseguenti alla violazione degli obblighi in materia di digitale ed è stata introdotta dal decreto-legge sulla governance del Piano nazionale di ripresa e resilienza (Pnrr) fra le disposizioni di accelerazione e snellimento delle procedure e di rafforzamento della capacità amministrativa (art. 41, comma 1, d.l. 31 maggio 2021, n. 77, convertito dalla legge 29 luglio 2021, n. 108), quindi pochi mesi prima che intervenisse la novella del 2021 sul d.lgs. n. 36/2006. Come intuibile, con l'articolo 18-*bis* del Cad il legislatore intende attrezzarsi con ulteriori strumenti per dare concreto seguito alla realizzazione delle misure di digitalizzazione della pubblica amministrazione italiana, realizzazione che consente l'erogazione dei finanziamenti europei nell'ambito del Pnrr. La procedura in caso di violazione degli obblighi di transizione digitale prevede un crescendo di azioni da valutarsi sulla base della gravità della violazione, azioni che possono arrivare all'applicazione delle sanzioni da parte di Agid, fino alla nomina di un commissario *ad acta* da parte del Presidente del Consiglio dei ministri o del Ministro delegato per l'innovazione tecnologica e la transizione digitale. Al riguardo è interessante osservare, anzitutto, come l'art. 12 del d.lgs. n. 36/2006 richiami espressamente la sola disposizione relativa alle sanzioni, ma non l'intero articolo 18-*bis* del Cad, con ciò volendo escludere la possibilità della nomina di un commissario *ad acta* per inadempienze più gravi. È degno di nota, inoltre, il fatto che le azioni previste dall'art. 18-*bis* del Cad e richiamate dalla disciplina sul riutilizzo non si applicano *tout court* a tutte le norme in materia di digitalizzazione, ma soltanto a specifiche disposizioni espressamente ivi elencate, come ad esempio quelle relative alla disponibilità dei dati delle pubbliche amministrazioni, contenute nell'art. 50 del Cad. La citata disposizione del Cad in materia di disponibilità dei dati, anche se non rinvia espressamente al d.lgs. n. 36/2006, come sopra già richiamato, stabilisce il riutilizzo dei dati detenuti dalle pubbliche amministrazioni da parte dei privati. Nell'ipotesi che l'amministrazione neghi al privato il riutilizzo dei propri dati, ci si chiede se il privato potrà tutelarsi non soltanto azionando gli strumenti a garanzia del diritto all'accesso, come stabilito dall'art. 5, comma 4 del d.lgs. n. 36/2006, ma anche attraverso gli strumenti di garanzia previsti per determinate disposizioni del Cad che, nel caso specifico, arrivano a prevedere la nomina del commissario *ad acta* (art. 50 e art. 18-*bis*, d.lgs. n. 82/2005). In altri termini, se l'istituto del riutilizzo è analizzato dal punto di vista del Cad, che lo disciplina all'articolo 50, ad esso sembrerebbero applicarsi tutte le forme di tutela del Cad introdotte per la realizzazione del Pnrr (ossia tutte le misure previste dall'art. 18-*bis* del Cad e non le sole sanzioni), che opererebbero per intero e non più soltanto limitatamente agli aspetti più tecnici definiti dalla normativa secondaria contenuta nelle linee guida Agid.

Per quanto premesso, è, dunque, possibile affermare che, sebbene le novelle del 2021 al d.lgs. n. 36/2006 abbiano il pregio di rendere maggiormente concreto il diritto al riutilizzo dell'informazione pubblica rispetto a quanto non venisse fatto in precedenza, risulterebbe, tuttavia, opportuna un'armonizzazione complessiva della disciplina anche con riferimento ai mezzi di tutela azionabili in caso di diniego.

6. Dati dinamici, dati di elevato valore, dati della ricerca

Una speciale disciplina è riservata ad alcune tipologie di dati, in particolare i "dati dinamici", le "serie di dati di elevato valore" e i "dati della ricerca". La direttiva 2019/1024 e il relativo decreto attuativo, oltre che il Regolamento di esecuzione 2023/138 forniscono, al riguardo, specifiche indicazioni alle pubbliche amministrazioni per consentire il riutilizzo di tali tipologie di dati.

I dati dinamici sono definiti come documenti informatici, soggetti ad aggiornamenti frequenti o in tempo reale, in particolare a causa della loro volatilità o rapida obsolescenza (art. 2, comma 1, lett. c-*sexies*, d.Lgs. n. 36/2006). Per comprendere esattamente cosa si intenda per dati dinamici è possibile far riferimento alla direttiva 2019/1024, dove si ribadisce che "i dati generati da sensori sono solitamente considerati dati dinamici" (art. 2, punto 8). I dati ambientali, relativi al traffico, satellitari

o meteorologici, come indicato nelle linee guida Agid, sono tutti esempi di dati dinamici. Tenuto conto della specifica natura dei dati dinamici, il legislatore stabilisce espressamente modi e tempi per il loro riutilizzo.

Altra novità della novella del d.lgs. n. 36/2006, operata per l'adeguamento alla nuova direttiva europea, consiste, nell'introduzione di "serie di dati di elevato valore". Le serie di dati di elevato valore sono documenti che, se riutilizzati, possono produrre importanti benefici per la società, l'ambiente e l'economia. Ciò poiché attraverso queste serie di dati si possono creare servizi, applicazioni a valore aggiunto, nuovi posti di lavoro dignitosi e di alta qualità, oppure poiché i servizi e le applicazioni basati su tali serie di dati hanno numerosi potenziali beneficiari (art. 2, comma 1, lett. c-*octies*), d.lgs. n. 36/2006 e art. 2, punto 10) della dir. 2019/1024). La direttiva europea fornisce sin da subito esempi di serie di dati di elevato valore: i codici di avviamento postale, le mappe e le carte nazionali e locali (dati geospaziali), il consumo energetico e le immagini satellitari (dati relativi all'osservazione della terra e all'ambiente), i dati provenienti da strumenti meteorologici (dati meteorologici), gli indicatori demografici e economici (dati statistici), i registri delle imprese e gli identificativi di registrazione (dati relativi alle imprese), la segnaletica stradale e le vie navigabili (considerando 66).

I dati della ricerca sono definiti – in modo equivalente dalla direttiva e dal decreto di recepimento – come "documenti informatici, diversi dalle pubblicazioni scientifiche, raccolti o prodotti nel corso della ricerca scientifica e utilizzati come elementi di prova nel processo di ricerca, o comunemente accettati nella comunità di ricerca come necessari per convalidare le conclusioni e i risultati della ricerca" (art. 2, comma 1, lett. c-septies), d.lgs. n. 36/2006 e art. 2, par. 9, direttiva 2019/1024). Il legislatore nazionale, quando definisce i dati della ricerca, non individua espressamente quali siano i dati che rientrino nella definizione, ma precisa anzitutto che sono esclusi quei dati, o, per meglio dire, quei documenti, che rientrano nelle pubblicazioni scientifiche. La direttiva 2019/1024, invece, fornisce esempi pratici di dati della ricerca, elencando nel considerando 27, fra gli altri, statistiche, risultati di esperimenti, misurazioni, osservazioni risultanti dall'indagine sul campo, immagini e registrazioni di interviste, oltre a metadati. Secondo la direttiva europea, pertanto, i dati statistici sono dati della ricerca e, in quanto tali, vanno messi a disposizione ai fini del riutilizzo. Il decreto di recepimento della direttiva in Italia, invece, non solo non indica espressamente i dati statistici fra i dati della ricerca, ma opera nei confronti dei dati statistici un'espressa esclusione (art. 3, comma 1, lett. g), d.lgs. n. 36/2006), richiamando la disciplina vigente in Italia in materia di segreto statistico (art. 9, d.lgs. n. 322/1989). Come osservato, non tutti i Paesi europei hanno introdotto nella loro legislazione il segreto statistico, che invece vige in Italia[42]. Con il Regolamento

42. Enrico Giovannini – economista e statistico, ex-Ministro dei governi Letta e Draghi, co-fondatore e Direttore scientifico dell'Alleanza Italiana per lo Sviluppo Sostenibile (ASviS) – in *Misurare il benessere oltre il PIL: nuove metriche per lo sviluppo sostenibile. L'importanza di sviluppare indicatori statistici non tradizionali*, webinar di ForumPA dell'11 dicembre 2024 (disponibile online nel sito di ForumPA), richiamando l'art. 3 del trattato dell'Unione europea che promuove il benessere dei suoi popoli, osserva come la legge di bilancio non ha alcun effetto su povertà, emissioni, disuguaglianze, ecc. In particolare, Giovannini affronta il tema di come coniugare la crescita del Pil con un benessere diffuso e ugualitario e segnala "un disallineamento grave della tempestività dei dati economici, sociali e ambientali". Riconosce che attraverso i sensori e i satelliti, l'aggiornamento dei dati ambientali ha fatto un balzo in avanti, ma restano indietro quelli sociali, che producono un problema serio, anche nella comunicazione. Secondo Giovannini, come accade in Olanda, quando l'Istat italiano pubblica i dati sul PIL annuale, dovrebbe poter mettere accanto anche altri indicatori, come l'occupazione di suolo, le diseguaglianze sociali, la disoccupazione, le emissioni, ecc., così da avere "una visione integrata tempestiva". L'Istat ovviamente provvede attraverso il suo annuario statistico e le pubblicazioni in materia a dare conto di questi aspetti, ma una cosa è parlarne congiunturalmente una cosa è parlarne separatamente. Questo richiede molto coraggio da parte della statistica pubblica, al quale la società civile potrebbe offrire un contributo importante, proponendo dei modelli economico/statistici basati sui dati. Ma Giovannini ricorda, al riguardo, che in Italia vi è una limitazione aggiuntiva causata non dall'Istat ma dal legislatore nell'uso dei microdati: la

di esecuzione della dir. 2019/1024, nell'armonizzare le caratteristiche tecniche dei dati degli Stati membri ai fini del loro riutilizzo, si introducono di fatto anche diverse serie di dati statistici, dal turismo alla fertilità, fra le serie di dati di elevati valore (allegato, punto 4, Reg. 2023/138), superando così, almeno per alcuni dati statistici, le limitazioni sopra richiamate sul segreto statistico. La direttiva, inoltre, stabilisce che i dati della ricerca finanziata con fondi pubblici dovrebbero essere resi aperti come opzione predefinita (considerando 28) e invita gli Stati membri a mettere a disposizione i dati della ricerca finanziata con fondi pubblici secondo i princìpi "FAIR" (art. 10, dir. 2019/1024). Il termine "fair", che dall'inglese potremmo tradurre come "corretto", "giusto", "equo" è un acronimo che sta per *findable, accessible, interoperable, reusable*. Il principio *findable* si riferisce alla reperibilità dei dati da parte di persone o macchine. Per l'attuazione del principio dell'accessibilità (*accessible*) occorre consentire l'accesso a dati e metadati a partire dall'identificatore univoco e persistente assegnato, utilizzare protocolli standardizzati e aperti (per es., http[43]) e rendere disponibili i metadati, anche quando i dati non sono immediatamente accessibili, perché, ad esempio, sono applicati meccanismi di autenticazione e autorizzazione all'accesso. In tal senso, il principio di accessibilità qui indicato non ha nessun legame con il principio di accessibilità previsto dalla legge Stanca (legge n. 4/2004), né tantomeno con il diritto di accesso sancito dalla legge in materia di trasparenza (legge n. 241/1990), ma si riferisce, invece, al fatto che è possibile fruirne grazie a una serie di accorgimenti tecnici (utilizzo di protocolli aperti, disponibilità dei metadati, ecc.). Il principio sull'*interoperabilità* richiede che i dati siano resi fruibili secondo la disciplina italiana ed europea in materia. Il principio *reusable*, infine, prevede che i dati siano ben documentati in modo da poter essere interpretati correttamente, replicati e/o combinati anche in contesti diversi.

7. Conclusioni

Il successo dello sviluppo dell'intelligenza artificiale in Europa, secondo il Parlamento europeo, dipende per buona parte dal successo della strategia europea sui dati[44]. L'Italia per quanto attiene all'apertura dei dati si è sempre collocata fra i Paesi europei più avanzati, confermando anche nel 2024 un'ottima posizione. La Commissione europea da dieci anni monitora il livello di maturità degli Stati membri nel campo dell'apertura dei dati, suddividendoli in quattro distinte categorie: "beginners", "followers", "fast-trackers" e "trendsetter"[45]. Per la misurazione sono presi a riferimento quattro elementi: le politiche sui dati, i portali, l'impatto e la qualità. Il nostro Paese, che nel 2024 complessivamente raggiunge una valutazione pari al 94%, superando la media europea dei 27 Stati membri che nel 2024 si attesta all'83%, risulta fra gli undici paesi "trendsetter", oscillando, negli ultimi cinque anni, fra l'ottava e la nona posizione. I dati italiani, in particolare, eccellono per la loro qualità, in quanto risulta che il portale italiano è il primo, tra quelli europei, per qualità dei suoi metadati. Si tratta di un risultato raggiunto partendo da un rating di "insufficiente", grazie all'encomiabile e sinergico lavoro dei colleghi di Agid con i fornitori e le singole pubbliche amministrazioni, che contribuiscono con i loro dataset a popolare il catalogo nazionale dati[46]. Ciò non vuol dire che i nostri dati siano già pienamente aperti e conformi alle specifiche europee, anche perché quello dell'apertura dei dati è un processo di miglioramento continuo[47]. Nell'analisi che l'Europa porta avanti per valutare lo sviluppo degli Stati membri nell'apertura dei

"*visione vecchia*" della legislazione italiana, che limita la capacità dell'Istat di condividere i dati con il mondo della ricerca, è un freno allo sviluppo di queste modellistiche che potrebbero supportare la statistica ufficiale.

43. *Hyper text transfer protocol* è il protocollo utilizzato per il funzionamento dei browser, che consente di visualizzare una pagina web sulla macchina client, inviando la richiesta a uno o più server che rispondono inviando i contenuti della pagina (cfr. Tanenbaum–Feamster–Wetherall 2023, p. 609).
44. European Parliament, Shaping the digital transformation: EU strategy explained, 2023.
45. *Open data maturity 2024 Italy*.
46. Agid, P*ortale Open Data, evoluzioni nel catalogo primo in Europa per qualità dei metadati*, 6 dicembre 2024.
47. Lo stato dell'arte dei dati pubblici italiani di elevato valore è descritto nella guida operativa Agid, cit., che, per ciascuna categoria e per ogni dataset indica azioni specifiche da adottare per la loro apertura, pp. 26-142.

dati da tempo è la Francia in testa alla classifica da ormai dieci anni. Probabilmente le ragioni del primato francese sull'apertura dei dati vanno ricercate nell'impegno anche politico che il Paese dimostra rispetto alla materia. L'apertura non solo dei dati, ma anche degli algoritmi e del codice sorgente dei servizi pubblici, infatti, costituisce una priorità del Primo Ministro francese e rappresenta il cuore della strategia di miglioramento del servizio pubblico, occupando grande spazio anche nel dibattito pubblico. Il Governo francese si pone l'obiettivo di mettere i dati al servizio dell'azione pubblica e individua le figure degli "amministratori di dati", uno per ciascuno dei propri quindici ministeri. La Francia, in questo modo, intende snellire le pratiche amministrative, stimolare l'innovazione e la creazione di nuovi servizi, migliorare l'efficacia delle politiche pubbliche, promuovere la trasparenza e facilitare il lavoro dei ricercatori, semplificando l'accesso ai dati pubblici, puntando, così, a mantenere la posizione di avanguardia mondiale in materia di sfruttamento dei propri dati pubblici[48]. In Italia, viceversa, l'apertura dei dati e il loro riutilizzo sono sempre stati inquadrati (per non dire "bollati") come una questione tecnica, fuori dall'agone politico, evento che, probabilmente, ne ha consentito uno sviluppo costante, favorendo il successo registrato a livello europeo.

Come indicato in premessa la competitività dell'Europa, come del nostro Paese, dipende dall'intelligenza artificiale e da come l'ingegno italiano ed europeo riusciranno a trarne il maggior valore. Nel suo piano d'azione per l'intelligenza artificiale del Continente la Commissione europea ha, fra l'altro, annunciato la presentazione di una strategia europea dei dati per l'Unione nella seconda metà del 2025, con l'obiettivo di rendere disponibili ancora più dati per l'IA e garantire un quadro giuridico semplificato, chiaro e coerente che consenta alle imprese e alle amministrazioni di condividere i dati senza soluzione di continuità e su larga scala, nel rispetto di elevati standard di privacy e sicurezza[49].

Oltre che dalla quantità dei dati, lo sviluppo dell'intelligenza artificiale dipende anche dalla qualità dei dati. Per aumentare la qualità dei dati, però, bisogna spingere verso una politica che non limiti l'uso del dato, ma lo incentivi, perché un maggiore utilizzo del dato produce anche un maggiore controllo sulla sua qualità. In tal senso, da un lato la diffusione delle buone pratiche delle amministrazioni e, dall'altro, l'auspicabile armonizzazione e semplificazione della normativa in materia, insieme allo sviluppo di competenze settoriali, potranno rappresentare importanti fattori per la continua innovazione dell'amministrazione italiana, che è alla base dell'innovazione del nostro Paese.

Riferimenti bibliografici

S. Aliprandi (2011), *Interoperability and Open Standards: The key to true openness and innovation*, in "The Journal of Open Law, Technology and Society", Vol. 3, 2011, n. 1

S. Calzolaio (2016), *Digital (and privacy) by default. L'identità costituzionale dell'amministrazione digitale*, in "Giornale di storia costituzionale", vol. 31, 2016, n. 1

E. Carloni (2022), *Il dovere pubblico alla trasparenza oltre i diritti di accesso e gli obblighi di pubblicazione*, in "Lo Stato", 2022, n. 19

G. Carullo (2025), *Dati, banche dati e interoperabilità dei sistemi informatici nel settore pubblico*, in R. Cavallo Perin, D.U. Galetta (a cura di), "Il diritto dell'Amministrazione Pubblica digitale", Giappichelli, 2025

48. Ministère de la transformation et de la fonction publiques, *Le Gouvernement poursuit son engagement pour une politique ambitieuse d'ouverture et d'exploitation des données publiques au service de l'action publique,* 23 maggio 2024.

49. European Commission, *AI Continent Action Plan – Q&A*.

C.M. Cascione (2005), *Il riutilizzo dell'informazione del settore pubblico*, in "Il diritto dell'informazione e dell'informatica", 2005

F. Costantino, M.L. Maddalena (2023), *Accesso ai documenti, trasparenza e intelligenza artificiale*, in "Diritto amministrativo", 2023

E. D'Orlando, G. Orsoni (2019), *Nuove prospettive dell'amministrazione digitale: Open Data e algoritmi*, in "Istituzioni del Federalismo", 2019, n. 3

D.U. Galetta (2019), *Open Government, Open Data e azione amministrativa*, in "Istituzioni del Federalismo", 2019, n. 3

I. Macrì (2021), *Open data, open format trasparenza e pubblicità dei dati delle Pubbliche Amministrazioni*, in "Azienditalia", 2021, n. 8-9

G. Mancosu (2019), *Les algorithmes publics déterministes au prisme du cas italien de la mobilité des enseignants*, in "Rivista italiana di informatica e diritto", 2019, n. 1

G. Mancosu (2016), *La transparence publique à l'ère de l'Open Data: Étude comparée Italie-France*, thèse de doctorat, Università degli Studi di Cagliari et Université Panthéon-Assas (Paris 2), a.a. 2014/2015

D. Martignago (2022), *Una governance dei dati genetici per lo sviluppo della ricerca scientifica*, in "Rivista italiana di informatica e diritto", 2022, n. 1

A. Monica (2024), *L'utilizzo degli Open Data per l'effettività dell'azione amministrativa nei procedimenti compositi europei (tra piattaforme digitali, intelligenza artificiale e space economy)*, in "CERIDAP", 2024, n. 2

V. Pagnanelli (2021), *Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali*, in "Rivista italiana di informatica e diritto", 2021, n. 1

P. Patrito, F. Pavoni (2012), *La disciplina del riutilizzo dei dati pubblici dal punto di vista del diritto amministrativo: prime riflessioni*, in "Il diritto dell'informazione e dell'informatica", 2012

M. Pietrangelo (2004), *Brevi note sul 'coordinamento informativo informatico e statistico dei dati dell'amministrazione statale, regionale e locale',* in "Informatica e diritto", 2004

B. Ponti (2006), *Il riutilizzo dei documenti del settore pubblico, commento al d.lgs. n. 36 del 2006*, in "Giornale di diritto amministrativo", 2006, n. 8

F. Sciacchitano (2018), *Disciplina e utilizzo degli Open Data in Italia*, in "Medialaws", 2018, n. 2

C. Sganga (2022), *Ventisei anni di direttiva database alla prova della nuova strategia europea dei dati: evoluzioni giurisprudenziali e percorsi di riforma*, in "Il diritto dell'informazione e dell'informatica", 2022, n. 3

A.F. Spagnuolo, E. Sorrentino (2022), *Open data per l'e-democracy*, in "Rivista italiana di informatica e diritto", 2022, n. 1

G. Strazza (2022), *I dati aperti in Italia: un focus sull'openness digitale dei Comuni*, in "federalismi.it", 28 dicembre 2022

A.S. Tanenbaum, N. Feamster, D. Wetherall (2023), *Reti di calcolatori*, Pearson, 2023

M. Wilkinson, M. Dumontier, I. Aalbersberg et al. (2016), *The FAIR Guiding Principles for scientific data management and stewardship*, in Sci Data 3, 160018 (2016)

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0248 • articolo sottoposto a peer review • pubblicato in anteprima il 5 dic. 2025

María Dolores García Sánchez

The virtual restraining order as a novel cyber precautionary measure to combat online crime

In light of the increasing digitalization of criminal conduct, the necessity of proportionate and effective precautionary measures has become a critical concern in contemporary criminal justice. Accordingly, this research explores the extent to which traditional precautionary frameworks can be adapted to address the unique challenges posed by cybercrime while ensuring compliance with fundamental rights. The examination of precautionary measures within the digital sphere, with particular emphasis on what we define as cyber-precautionary measures, constitutes a fundamental aspect of contemporary criminal justice. This study adopts a progressive analytical approach, commencing with a general overview of this emerging category of precautionary measures in criminal proceedings before advancing to an in-depth analysis of a novel proposal: the virtual restraining order. The research further investigates the technical and legal feasibility of this new cyber-precautionary measure, as well as the role of Internet Service Providers in implementing it. Subsequently, the discussion will focus on the specific legal and practical dimensions of this measure, with particular attention to its implications for fundamental rights, the principle of proportionality, and its practical implementation.

Cyber-precautionary measures – Cybercrime – Virtual restraining order – Fundamental rights – Proportionality

L'ordine di allontanamento virtuale come nuova misura cautelare cibernetica per combattere il crimine online

Alla luce della crescente digitalizzazione delle condotte criminali, la necessità di misure cautelari proporzionate ed efficaci è diventata una questione cruciale nella giustizia penale contemporanea. Di conseguenza, questa ricerca esplora quanto le misure cautelari tradizionali possano essere adattate per affrontare le sfide uniche poste dalla criminalità informatica, garantendo al contempo il rispetto dei diritti fondamentali. L'analisi delle misure cautelari nell'ambito digitale, con particolare enfasi su quelle che definiamo misure cibernetiche, costituisce un elemento fondamentale della giustizia penale contemporanea. Questo studio adotta un approccio analitico progressivo, partendo da una panoramica generale di questa categoria emergente di misure cautelari nei procedimenti penali, per poi approfondire una proposta innovativa: l'ordine di restrizione virtuale. La ricerca esamina inoltre la fattibilità tecnica e giuridica di questa nuova misura cibernetica cautelare, nonché il ruolo dei fornitori di servizi Internet nella sua attuazione. Successivamente, la discussione si concentrerà sugli aspetti giuridici e pratici specifici di questa misura, con particolare attenzione alle sue implicazioni per i diritti fondamentali, il principio di proporzionalità e la sua applicazione pratica.

Misure cautelari cibernetiche – Criminalità informatica – Ordine di allontanamento virtuale
Diritti fondamentali – Proporzionalità

The author is Postdoctoral Research Professor at the University of Seville, Spain

The present study has been conducted within the framework of the 2021 Predoctoral Grant (PAIDI 2020), funded by the Regional Ministry of Economic Transformation, Industry, Knowledge, and Universities of the Government of Andalusia (PREDOC_02268)

1. Introduction

The increasing digitalization of criminal conduct has exposed the limitations of precautionary frameworks traditionally designed for an analog and territorially bounded environment. Whereas classical precautionary measures target individual's personal freedom or economic assets, the dynamics of cyberspace – characterized by anonymity, deterritorialization, and ubiquity – demand novel responses capable of addressing new forms of victimization and safeguarding the integrity of digital evidence. This evolving landscape calls for the reconceptualization of precautionary action, moving beyond conventional instruments to a set of cyber-precautionary measures specifically tailored to the challenges of online crime.

The present study introduces the proposal of a virtual restraining order as a distinctive cyber-precautionary measure. The aim of this instrument is to restrict an investigated individual's access to certain digital spaces in order to prevent reoffending, reduce impunity, and reinforce the protection of victims' rights in the online sphere.

The relevance of this proposal lies not only in its pragmatic orientation but also in its theoretical contribution to the debate on the modernization of criminal procedure in the digital age. By examining its legal feasibility, proportionality requirements, and practical implementation this study seeks to evaluate the potential of the virtual restraining order to operate as a proportionate and rights-compliant response to cybercrime. In doing so, it aims to contribute to the broader discussion on how criminal justice systems can adapt to technological transformations without compromising fundamental rights.

Accordingly, this research seeks to answer the following question: to what extent can the introduction of a virtual restraining order be framed as an effective and legally viable cyber-precautionary measure that complies with the principle of proportionality in combating cybercrime? Addressing this question requires an interdisciplinary perspective that combines doctrinal analysis, jurisprudential developments, and technological considerations.

The paper is structured as follows. First, it sets out the methodological premises, describing the analytical approach and the sources of law and doctrine employed. Second, it offers preliminary considerations, delimiting the concept of cyber-precautionary measures as a new category distinct from traditional mechanisms. Third, it develops the central proposal of the virtual re-

straining order, examining (a) its definition and nature, (b) its implications for fundamental rights and the principle of proportionality, including the necessity of judicial authorization, and (c) the technical and practical aspects of its implementation, with specific reference to the role of Internet Service Providers. Finally, the article presents its conclusions, evaluating the feasibility, limitations, and potential contributions of the measure to the modernization of criminal procedural law in the digital environment.

2. Methodological premises

This study undertakes a comprehensive examination of precautionary measures within the realm of cybercrime, with a particular focus on the adoption and legal implications of cyber-specific precautionary mechanisms such as the virtual restraining order.

Methodologically, for this research we employ an analytical and deductive approach, progressing from a general overview of precautionary measures in criminal proceedings to an in-depth assessment of their applicability to cybercrime cases. Additionally, we adopt a critical and proactive stance, aiming not only to assess current regulatory and jurisprudential developments but also to propose concrete legal and technical solutions to enhance the effectiveness of this virtual restraining order as a cyber-precautionary measure. A central emphasis is placed on the principle of proportionality as the guiding criterion for evaluating the necessity, suitability, and proportionality in the strict sense of digital restrictions.

In terms of methodological techniques, our study relies primarily on jurisprudential analysis, ensuring a thorough examination of relevant judicial decisions at the national, European and international levels. This is complemented by an extensive review of legal texts, including the Spanish Constitution, organic and ordinary laws, European regulations, and pertinent international treaties. Furthermore, by integrating recent academic discourse on digital evidence, cybersecurity, and judicial cooperation this research aims to contribute to the ongoing legal and theoretical debate on the adaptation of precautionary measures to the evolving landscape of cybercrime.

3. Preliminary considerations: cyber-precautionary measures as a new category of precautionary measures

The distinctive characteristics of digital interactions – particularly anonymity, ubiquity, and deterritorialization – have facilitated the rapid expansion of new forms of criminal activity in cyberspace. As a dynamic and adaptive normative system, Law must provide effective responses to these evolving criminological challenges. Such adaptation must occur in parallel with technological advancements, addressing the inherent risks and threats they entail.

In a globalized world, the absence of physical boundaries in cyberspace enables the commission of crimes beyond geographical borders, underscoring the need for transnational prevention and prosecution strategies. These strategies must overcome jurisdictional fragmentation and reduce impunity. The complexity of investigating and prosecuting cybercrimes, coupled with their high impunity rates[1], highlights the importance of prevention and the adoption of precautionary measures suited to the digital landscape. Consequently, precautionary regulations must be tailored to the specific challenges of cyberspace and the demands of a technologically evolving society. The dynamic nature of cybercrime requires a flexible and effective precautionary framework aimed at preserving digital evidence, preventing recidivism, and protecting victims throughout the criminal process.

Within this context, an expanded and redefined concept of precautionary measures emerges, specifically adapted to the peculiarities of cybercrime. Traditional precautionary measures, designed for the physical world, are primarily aimed at restricting individuals, either through limitations on personal freedom or on economic assets. By contrast, in the online environment, the immediate object of criminal conduct lies in digital elements – such as data, content, communication channels, or online platforms – that require a different form of intervention. This mismatch highlights the need for a new category of instruments: cyber-precautionary measures.

Cyber-precautionary measures encompass those adopted in response to illicit conduct per-

1. The "unrecorded" crime rate.

petrated in cyberspace, facilitated by or involving the use of the Internet and ICTs. Given the altered spatiotemporal parameters of this digital realm, these measures are conceptually distinct from conventional precautionary mechanisms designed for the analogue world. Their defining feature rests upon their function: to block, restrict, or remove unlawful digital content, ensuring its preservation for judicial purposes, while simultaneously protecting victims from the ongoing harm and revictimization associated with its continued availability online.

At first glance, the conceptual distinction appears straightforward: while traditional precautionary measures are person-oriented, cyber-precautionary measures are object-oriented, focusing on illicit electronic content or virtual spaces rather than directly on the alleged offender. However, this distinction requires careful refinement. Although cyber-precautionary measures are formally directed at digital "objects" (e.g., unlawful data, websites, or platforms), the implementation of certain measures may indirectly entail restrictions on individuals, since human interaction is the medium through which such digital objects are accessed, disseminated, and operationalized.

This tension becomes particularly evident in the case of the novel virtual restraining order we propose in this study (which will be examined in greater detail below). It represents the clearest point of friction between the person-oriented logic of traditional precautionary measures and the object-oriented nature of cyber-precautionary interventions. As a precautionary order, it must be issued against a specific individual and therefore retains an unavoidable personal dimension. Yet, its operational content remains object-centered: what is restricted is not the individual's ambulatory freedom, but their capacity to access, generate, or interact with defined digital spaces and electronic content. In other words, the measure targets the virtual space (the "object"), while its personal consequences materialize only as a derivative effect (namely, the prohibition of accessing that environment). This dual structure is unique to virtual restraining orders and explains why they occupy a hybrid conceptual position within the broader category of cyber-precautionary measures.

By contrast, other cyber-precautionary instruments – such as content removal, blocking orders, or data preservation – can be adopted even in the absence of an identified suspect, since their aim is to neutralize the circulation, persistence, or evidentiary vulnerability of illicit digital content. Such measures thus confirm the autonomous object-orientation of cyber-precautionary action and clearly differentiate it from the traditional framework, where precautionary powers are primarily exercised upon the person in the analogue sphere.

On this basis, the apparent conceptual tension does not undermine the coherence of cyber-precautionary measures, provided that their objectivization is explicitly articulated. The key differentiating factor is not the total absence of personal impact, but the locus of the legal intervention: whereas traditional precautionary measures directly curtail personal liberty in the physical world, cyber-precautionary measures operate in the digital domain, acting upon electronic data, online infrastructures, and virtual environments, with personal restrictions arising only as a secondary and indirect consequence. This object-centered and digitally-grounded design aligns with the structural aims of contemporary criminal procedure in cyberspace, where the urgency lies in preventing the dissemination of illicit content, preserving digital evidence, and mitigating ongoing victimization.

From this perspective, cyber-precautionary measures align with an expanded conception of precautionary action characterized by a dual function: (1) an evidentiary-preservation function, aimed at preventing the destruction or alteration of digital evidence, and (2) a preventive and restorative protective function, designed to halt or mitigate criminal activity while safeguarding the rights and interests of victims.

Given their potential to affect freedom of expression, privacy, and Internet access, cyber-precautionary measures must operate under the principle of proportionality, which functions as both a limiting and legitimizing norm.

Specifically, the proportionality test entails three cumulative requirements[2]: (1) Suitability, whereby the measure must be capable of achieving its legitimate aim; (2) Necessity, ensuring that no less intrusive

2. See , SSTC 66/1995; 55/1996; 207/1996;152/1996.

alternative exists; and (3) Proportionality *stricto sensu*, demanding that the interference with rights not exceed what is strictly required to meet its objectives.

This principle establishes a stringent threshold of judicial justification for any restriction of digital liberties. Accordingly, precautionary measures must be narrowly defined, exceptional in scope, and subject to continuous judicial oversight. Their legitimacy depends on a demonstrable connection between the imposed limitation and the protection of compelling public interests, notably the preservation of digital evidence and the prevention of further victimization.

As Alexy[3] has emphasized, proportionality transforms judicial discretion into a structured reasoning process, enhancing transparency, rationality and normative coherence. Likewise, Jackson[4] points out that proportionality operates as a *bridge principle* between decision making in courts and decision making by the people, legislatures and public officials. This interpretative framework ensures that the exercise of coercive state powers in the digital domain remains anchored in constitutional guarantees, even amidst rapidly evolving technological contexts.

Thus, proportionality not only circumscribes the reach of cyber-precautionary powers but also legitimizes them when strictly necessary to preserve digital evidence, prevent reoffending, and protect victims from renewed harm. In this dual role – constraint and justification – the principle stands as the doctrinal keystone of a precautionary model suited to the complex normative demands of the digital age.

Ultimately, the fight against cybercrime demands an updated precautionary framework capable of effectively addressing the distinctive challenges of the digital environment. Without a prompt and reinforced precautionary system, the effectiveness of investigative techniques is severely compromised, resulting in heightened levels of impunity and diminished victim protection. The evolution of cybercrime necessitates moving beyond outdated regulatory frameworks and advancing toward a precautionary model suited to the complexities of the digital age.

Within the Spanish legal framework, cyber-precautionary measures include those established under Article 13.2 of the Criminal Procedure Act (LECrim), which provide for content removal, access blocking, and service suspension, as well as the data preservation order set forth in Article 588-*octies* LECrim. However, given the rapid advancement of technology and the corresponding evolution of cybercriminal tactics, additional precautionary measures of this nature are required. Specifically, we propose the introduction of a "virtual restraining order", designed to restrict an investigated individual's access to specific digital spaces or online platforms associated with the victim or the offence. The conceptualization and development of this measure will be the focus of the following sections.

4. The virtual restraining order as a novel cyber-precautionary measure

4.1. Definition

The virtual restraining order can be defined as a measure designed to restrict contact, access to existing online content, or the generation of illicit online material by limiting the use of the medium through which the alleged criminal act is committed (namely, the Internet). It operates as a preventive mechanism intended to protect victims and prevent reoffending in cases where online interaction constitutes the means or context of the offence. This measure is particularly relevant in cases of cyberstalking, cyberbullying, and other unlawful behaviors perpetrated through digital means.

In Spain, the Supreme Court (TS) has provided a jurisprudential interpretation of restrictions on contact in the online sphere. Specifically, ruling 547/2022, of June 2, extends the prohibition of "contacting by any means" with the victim to include restrictions on the defendant's access to "computer locations" frequented by the victim. A detailed analysis of this ruling and its implications will be addressed later.

However, the novel precautionary measure proposed here offers an additional level of protection for victims and contributes to the prevention of repeat offenses. Firstly, it would not rely solely on jurisprudential interpretation, thereby providing greater legal certainty through the establishment of clearly defined conditions, requirements, and

3. Alexy 2002.
4. Jackson 2015.

principles for its application within the legal framework. Moreover, this virtual restraining order would extend beyond direct communication between the accused and the victim to encompass virtual spaces frequented by the victim, even in the absence of explicit interaction. The mere simultaneous presence of both parties in the same digital environment could suffice to activate the order. In this context, the psychological and relational dimension of harm[5] experienced by victims emerges as a core justificatory axis of the measure. The persistence of illicit material online or unwanted digital proximity with the offender can generate a form of continuous victimization, extending the effects of the original offence well beyond its initial commission[6]. Even without direct contact, the awareness of the offender's online presence may inhibit the victim's willingness to participate freely in digital spaces, producing a chilling effect on their autonomy and communicative self-determination. Such dynamics reveal how virtual coexistence can perpetuate relational coercion despite the absence of physical contact, thereby justifying a tailored precautionary intervention. Against this backdrop, the virtual restraining order extends protection within the digital sphere, offering more robust and context-sensitive safeguards than the current jurisprudential interpretation of "contact by any means". By targeting the digital spaces in which psychological pressure or symbolic intrusion occurs, the measure operates as both a preventive mechanism – reducing the risk of reoffending – and a restorative instrument, aimed at re-establishing the victim's sense of safety, autonomy, and digital dignity.

As regards the rationale underpinning the new precautionary measure, its foundation is twofold. On the one hand, it acknowledges that unrestricted Internet access for an individual under criminal investigation may seriously hinder efforts to prevent reoffending and to safeguard the victim's legal interests. As a precautionary measure rather than a penalty, the virtual restraining order effectively serves these objectives while preserving the integrity of the legal process. The interactive, decentralized and instantaneous nature of digital communication, renders *ex ante* control over illicit content neither feasible nor desirable. Consequently, regulatory intervention in cyberspace must focus on controlling access to the specific digital contexts where harm is generated or perpetuated. Within this framework, the virtual restraining order would, therefore, target those digital environments identified by judicial authorities as relevant to the alleged conduct, ensuring both proportionality and technological feasibility. On the other, as a procedural safeguard, the virtual restraining order embodies the principle of *ultima ratio*, intervening only where less intrusive alternatives prove inadequate to guarantee effective victim protection or the preservation of digital evidence.

In practical terms, enforcement of this measure would require collaboration between judicial authorities, Internet Service Providers (ISPs), and technical experts. Its implementation could involve the installation or execution of monitoring or blocking software on the devices used by the investigated individual, configurated to:

- prevent any form of contact with the victim, in the broad sense outlined above;
- restrict access to online platforms or websites habitually visited by the victim;
- limit the use of social networks or applications associated with the alleged conduct;
- apply other technically feasible restrictions necessary to prevent recidivism and protect the victim's rights in the digital environment.

This measure seeks to prevent reoffending concerning the protected legal interest, whether personal (as in offenses against honor or privacy) or collective (such as terrorism-related crimes or the distribution of child pornography).

It is important to clarify that a "virtual restraining order" does nor replicate the legal nature of a traditional restraining order, which limits physical proximity or ambulatory freedom. Instead, it operates through a digital analogue: a calibrated limitation on the individual's interaction with specific online environments identified as vectors of potential harm[7]. As such, it affects a distinct sphere of liberty: the freedom of expression and

5. See, Bettiga 2020, Martellozzo–Jane 2017.
6. Agustina Sanllehí–Gámez-Guadix–Montiel Juan, 2020.
7. It is important to remember that the virtual restraining order primarily targets electronic content and data, namely, the digital spaces, platforms, and communication channels where illicit conduct may be reproduced,

the right to Internet access, as the latter serves as a prerequisite for exercising the former through digital platforms[8]. Given its potential impact on these fundamental freedoms, its adoption must always undergo a proportionality assessment, ensuring necessity, suitability and proportionality *stricto sensu*, as further discussed in the subsequent section.

Ultimately, the virtual restraining order reflects the evolution of precautionary logic in the digital era: it's a forward-looking and technologically adapted mechanism, reconciling preventive protection with procedural guarantees. By combining technological feasibility, judicial oversight, and a proportional rights-based approach, it seeks to balance the imperatives of victim protection with the foundational principles of the rule of law in cyberspace.

4.2. Fundamental rights, proportionality principle, and the need for judicial authorization

4.2.1. Fundamental rights

As stated above, the implementation of such a precautionary measure inevitably affects fundamental rights, particularly freedom of expression and the right to Internet access. More broadly, such restrictions impinge upon the right to access technology, which has become an essential component of personal development and social inclusion in the information society[9].

The increasing significance of Internet access and digital connectivity is closely associated with what scholars describe as the emerge of a fourth generation of human rights[10], shaped by technological progress and the rise of informational autonomy. However, the extent of its legal recognition remains fragmented. Some jurisdictions have enshrined Internet access constitutionally, while others recognized it through judicial interpretation, statutory provisions, or soft-law[11].

At the international level, the United Nations (UN) has explicitly affirmed the human right to Internet access as intrinsically linked to freedom of expression and information. The UN Human Rights Council Resolution of 5 July 2018 on the *Promotion, Protection, and Enjoyment of Human Rights on the Internet*[12] declares that "the same rights people have offline must also be protected online;", thereby recognizing the Internet as a structural condition for democratic participation. The UN General Assembly Resolution of

disseminated, or perpetuated. The resulting limitation on the investigated person's conduct emerges only as an indirect consequence of this object-oriented intervention.

8. Aslam–Kaaniru–Abiero 2025.

9. In particular, as Rodotà points out: "Il diritto di accesso a Internet, tuttavia, va inteso non solo come diritto a essere tecnicamente connessi alla rete, bensì come espressione di un diverso modo d'essere della persona nel mondo, e dunque come effetto di una nuova distribuzione del potere sociale. (…) Il diritto di accesso, infatti, si presenta ormai come sintesi tra una situazione e l'indicazione di una serie tendenzialmente aperta di poteri che la persona può esercitare in rete". See , Rodotà 2012. On the other hand, in Frosini's view, "Il diritto di accesso a Internet è da considerarsi un diritto sociale, o meglio una pretesa soggettiva a prestazioni pubbliche, al pari dell'istruzione, della sanità e della previdenza. Un servizio universale che le istituzioni nazionali devono garantire ai loro cittadini attraverso investimenti statali, politiche sociali ed educative, scelte di spesa pubblica. Infatti, sempre di più l'accesso alla rete Internet, e lo svolgimento su di essa di attività, costituisce il modo con il quale il soggetto si relaziona con i pubblici poteri, e quindi esercita i suoi diritti di cittadinanza". See, Frosini 2011. In the same vein, the Council of Europe, in its Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to Human Rights for Internet UsersRecommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to Human Rights for Internet Users (adopted on April 16, 2014), recognizes that access to the Internet is an important means of exercising rights and freedoms, as well as participating in democracy. For this reason, it must be "affordable and non-discriminatory".

10. Bustamante Donas 2001; Bustamante Donas, 2010; Acata Águila 2011; Riofrío Martínez Villalba 2014; Morales Aguilera 2018; León Camacho 2020; Cova Fernández 2022.

11. Álvarez Robles 2022.

12. United Nations (2018), The promotion, protection and enjoyment of human rights on the Internet,The promotion, protection and enjoyment of human rights on the Internet, (A/HRC/RES/38/7), July 5, 2018.

13 July 2021[13] further deepened this perspective, highlighting Internet access as indispensable for education, employment, healthcare, and civic engagement, and urging States to ensure open, reliable, and secure connectivity while combating disinformation and hate speech within a human rights – compliant framework.

The COVID-19 pandemic reinforced the essential nature of Internet access in contemporary society, prompting the UN to explore its potential incorporation into binding international legal frameworks[14].

In the European context, the European Court of Human Rights (ECHR) addressed this issue in *Ahmet Yildirim v. Turkey* (Judgement of 18 December 2012). The ruling acknowledged that the right to Internet access is inherent to the right to access information and communication, as protected by national constitutions. It further established that this right entails both individual participation in the information society and a state obligation to ensure Internet access for citizens[15]. This judgment underscores the constitutional protection of Internet access due to its direct link to freedom of expression and information.

However, the ECHR also clarified that Internet access is not an absolute right, as its exercise may be lawfully restricted to serve overriding interests, such as crime prevention and law enforcement. Accordingly, any limitations must be proportionate and strike a balance between competing legal interests[16].

The Court of Justice of the European Union (CJEU) has similarly addressed Internet access within the framework of data protection (Article 16.1 TFEU and Article 8.1 CFR)[17] and digital market regulation. In its judgment of September 15, 2020[18], the CJEU interpreted Regulation 2015/2120[19] for the first time, establishing the principle of net neutrality and recognizing that unduly restricting access to online content or services infringes both the freedom to conduct a business and user's right to information. This jurisprudence positions Internet access as an instrumental right indispensable to the enjoyment of other freedoms protected under EU law.

Consequently, Internet access has thus evolved into an instrumental right, essential for the effective exercise of other fundamental rights, including education, employment, healthcare, and access to information. In the context of the ongoing technological and digital transformation, unrestricted access to the Internet is fundamental to personal development and human dignity. In the 21st century, where most interactions take place online[20], digital exclusion due to lack of Internet access can lead to social marginalization, exacerbating existing inequalities and hindering full participation in modern society[21].

13. United Nations (2021), The promotion, protection and enjoyment of human rights on the Internet,The promotion, protection and enjoyment of human rights on the Internet, (A/HRC/RES/47/16), July 13, 2021.
14. United Nations (2020), Covid-19 makes universal digital access and cooperation essential: UN tech agencyCovid-19 makes universal digital access and cooperation essential: UN tech agency, May 2, 2020.
15. ECtHR (Second Section), December 18, 2012. *Yildirim v. Turkey*, application no. 3111/10, paragraph 31.
16. ECtHR, (Fourth Section), December 2, 2008, *K.U. v. Finland*, application no. 2872/2002.
17. Of particular significance in our constitutional context at this point is the *Google Spain* ruling (CJEU, Grand Chamber, May 13, 2014, case C-131/12).
18. Judgment in the joined cases C-807/18 and C-39/19 *Telenor Magyarország Zrt./Nemzeti Média- és Hírközlési Hatóság Elnöke*.
19. Regulation (EU) 2015/2120 of the European Parliament and of the Council, laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (November 25, 2015).
20. Nannipieri 2013; Frosini 2011; Pisa 2010.
21. "In a world more and more based on economic and social electronic networks, the right not to be excluded the right to access acquires an increasing importance. Concepts like 'inclusion' and 'access' have today replaced those (corresponding) of autonomy and possession, which characterized the notion of property in a traditional sense: in the new economy, the concept of property does not refer to a power of excluding others from enjoying personal goods anymore, rather it qualifies as a right to not be excluded from the society's resources".

Comparative constitutional experiences further illustrate this normative trajectory.

In Mexico, the 2013 amendment to Article 6 of its Constitution expressly guarantees citizens the right to access and use ICTs in everyday life, obliging authorities to promote universal connectivity[22].

In other jurisdictions, this right has been established through judicial precedent. In France, the Constitutional Council (Decision No. 2009-580 DC, June 10, 2009) recognized Internet access as a fundamental right, distinct from freedom of thought and opinion enshrined in Article 11 of the 1789 Declaration of the Rights of Man and of the Citizen. Drawing on this comparative legal foundation, the Constitutional Chamber of the Supreme Court of Justice of Costa Rica subsequently ruled in favor of Internet access as a fundamental right[23].

By contrast, some States have opted for a legislative approach. On July 1, 2010, Finland passed a law recognizing Internet access as a legal right[24]. Similarly, Italy, through the Legge Stanca of January 9, 2004[25], linked access to digital services with the principle of equality (Article 3 of the Italian Constitution), emphasizing accessibility for persons with disabilities[26].

In Spain, Internet access enjoys statutory recognition under Article 81 of Organic Law 3/2018 on Data Protection and Digital Rights, which mandates universal, affordable, high-quality, and non-discriminatory connectivity. The Digital Rights Charter[27], although not binding, reinforces the State's responsibility to guarantee effective, equitable access and prevent digital exclusion. The General Telecommunications Law[28] (Law 11/2022, June 28) further strengthens this right by defining its minimum essential content[29], which include access to email services; search engines; basic online training and education tools; online news or press; e-commerce platforms; job search portals and professional networking; Internet banking; e-government services; social networking and instant messaging; and telephone and video calls (standard quality).

Given the above, this law could serve as a foundation for the constitutional recognition of Internet access as a fundamental right[30], analogously to the right to be forgotten, which emerged from the constitutional protection of data (Article 18.4 CE). Under this approach, a constitutional embodiment of this right could be achieved by linking it to the right to data protection (Article 18.4 CE), freedom of expression and information (Article 20 CE) and the right to communicate and receive truthful information by any means of dissemination[31] (Article 20 CE) [32], thereby affirming the digital dimension of citizenship.

In short, through a systematic interpretation of these pre-existing fundamental rights, the fundamental character of Internet access could be established.

See , Rifkin 2000.

22. Comisión Nacional de los Derechos Humanos. Instituto Nacional de Estudios Históricos de las revoluciones de México, Derecho de acceso y uso de las tecnologías de la información y la comunicación, Biblioteca Constitucional CNDH-INEHRM, November 2015.
23. Ruling 12790-2010.
24. Miranda Bonilla 2016.
25. Known by this name after its promoter, Lucio Stanca.
26. Pollicino–Romeo 2016.
27. *Carta de Derechos Digitales*, in "Web oficial del presidente del Gobierno y el Consejo de Ministros", 2021.
28. Ley 11/2022, de 28 de junio, General de Telecomunicaciones, 2022.
29. According to Art. 37 in connection with Annex III.
30. Álvarez Robles 2024.
31. Frosini expands on this idea, arguing that a constitutional right to Internet access is being created at the jurisprudential level. In the context of widespread Internet diffusion, the freedom of communication and expression necessarily presupposes the freedom to access such online communication services, and it is the obligation of states to eliminate obstacles that, in practice, prevent the exercise of such universal service for all citizens. See, Frosini 2011.
32. Spanish Constitutional Court, rulings 31/2010, 8/2012, 8/2016 y 20/2016.

In particular, a constitutional recognition of Internet access as a fundamental right should entail, at a minimum, the prohibition of prior and collateral censorship, a ban on indiscriminate and arbitrary filtering, monitoring, or control mechanisms and protection against interference with content[33], including generalized blocking or interruptions of Internet services[34].

Any restrictions should be imposed only retrospectively, subject to the legality of the content in question[35]. However, until this right attains fundamental status, it remains structurally fragile, lacking both direct enforceability against public authorities and a reinforced system of legal guarantees that would allow individuals to enforce its protection before the courts[36].

In conclusion, the consolidation of a constitutional right to Internet would serve as a normative cornerstone for future digital precautionary measures. It would ensure that any restriction – such as the virtual restraining order proposed herein – operates within a framework of legality, necessity, and proportionality, thereby harmonizing individual rights, technological progress, and the preventive aims of criminal justice in the digital age.

4.2.1.1. The concept of the "computer domicile" and its implications for virtual restraining measures

At this juncture, it is pertinent to examine the legal implications of safeguarding what some jurisdictions refer to as the "computer domicile" when imposing cyber precautionary measures, such as a virtual restraining order. This concept, which has no direct equivalent in Spanish law, has been particularly developed in German and Italian jurisprudence.

In Germany, the term "computer domicile" is used to designate the virtual space where individuals or entities conduct online activities. A landmark ruling by the German Constitutional Court in 2008 played a pivotal role in this regard[37]. Faced with the challenges posed by covert surveillance of information systems, the Court found it insufficient to rely solely on an evolutionary interpretation of constitutional guarantees concerning the confidentiality of telecommunications, the inviolability of the home, and the right to informational self-determination. As a result, the Court explicitly recognized – for the first time in Europe[38] – a new fundamental right of constitutional rank: the "right to the integrity and privacy of information systems". This right ensures that the so-called "digital citizen" can freely and securely use information and communication technologies[39]. Subsequent rulings by the German Constitutional Court upheld the admissibility of digital investigative measures allowing remote data acquisition, provided they adhered to the principle of proportionality, ensuring a balance between protecting this newly recognized right and other competing legal interests and judicial oversight requirements, to prevent excessive state interference[40].

33. Except for those causes strictly provided for by law (principle of legality). See, García Mexía 2018.
34. Álvarez Robles 2022.
35. Velasco Núñez 2012.
36. In particular, that it can be challenged through the "amparo" appeal before the Constitutional Court (Article 53 CE), with direct effectiveness and development through Organic Law.
37. Decision of the German Federal Constitutional Court (BVerfG) of February 27, 2008, in which it was called upon to assess the legitimacy of a provision in the North Rhine-Westphalia State Constitution Protection Law, which allowed a government intelligence agency to conduct surveillance and secret access to networked computer systems.
38. Venegoni–Giordano 2016.
39. The German Constitutional Court, therefore, declared the unconstitutionality of the regulation that provided for the surveillance of computer systems as an intelligence activity in relation to the new fundamental right. However, it did not completely exclude the possibility of allowing such monitoring as an investigative tool. See, Torre 2015.
40. BVerfG, April 20, 2016, where the Court reaffirmed the compatibility of covert surveillance measures by the police with the fundamental rights recognized by the Constitution, in order to protect society from the threats of international terrorism. However, some provisions of the contested federal law – regulating the activities of

In Italy, references to the "computer domicile" have also emerged in legal discourse. However, before analyzing this concept, it is essential to distinguish it from the "digital domicile" (*domicilio digitale*[41]), as the two terms hold distinct legal meanings.

The "digital domicile" refers to a certified email address[42] that holds legal validity for official electronic communications. It can be voluntarily chosen by individuals upon reaching legal adulthood, but it is mandatory for certain legal entities and professionals. Since July 6, 2023, any individual in Italy can access another person's electronic domicile without prior authorization[43] by entering their *codice fiscale* (tax identification number) into a designated public platform. By contrast, the "computer domicile" – which is relevant for criminal law protections – refers to the virtual space where fundamental freedoms such as privacy, freedom of communication, and freedom of expression are exercised. This concept is characterized by its dynamic, mobile, and evolving nature, as digital technologies enable continuous access to sensitive data from multiple locations.

In particular, the Italian Court of Cassation has defined the "computer domicile" as the digital space where personal data is stored, protected by security measures such as passwords or encryption keys. This space, the Court has ruled, merits legal protection against unauthorized intrusions in the same manner as an individual's private sphere[44].

This protection is codified in Article 615-*ter* c.p. (Italian Penal Code)[45], which criminalizes: "Anyone who unlawfully accesses a computer or telematic system protected by security measures or remains within it against the express or implied will of the rightful owner". The decision to classify this offense alongside violations of the physical home's inviolability (Article 614 c.p.) underscores the legislative intent to equate the legal protection afforded to both physical and digital domiciles[46].

Traditionally, in procedural criminal law, the notion of "place" has been linked to a defined physical space. This conceptualization is relatively straightforward when applied to a tangible computing device, which occupies a specific location and serves as a data storage medium. As a result, digital devices are often treated as "places" for the purposes of criminal investigations, much like physical premises where searches and seizures are conducted. However, determining whether a virtual space within a network can also be regarded as a "place" presents significant legal challenges. The materiality that traditionally defines a "place" in the physical world cannot be strictly transposed to cyberspace, given its inherently fluid, decen-

the federal police and cooperation in criminal matters between state and federal governments, as well as with third countries – were declared unconstitutional for violating the principle of proportionality in the balance between public powers and individual prerogatives. See, Venegoni–Giordano 2016.

41. This figure also exists in Argentina (Article 40 of the Civil and Commercial Procedural Code of the Province of Buenos Aires, amended by Law 14.140). Specifically, the Diccionario panhipánico del español jurídicoDiccionario panhispánico del español jurídico defines it as "A domicile that replaces or coexists with the physical domicile established in the judicial file, to which all notifications that should not be sent to the actual domicile must be directed".
42. Known as "Posta elettronica certificata" (PEC) in Italy.
43. "Indice Nazionale dei Domicili Digitali" (INAD).
44. Cass., Sez. VI, 14 dicembre 1999, n. 3067, in "Cassazione Penale", 2000.
45. Introduced by Law No. 547/1993.
46. In an initial ruling, the Tribunale di Torino, Sez. IV penale, 7 febbraio 1998, already affirmed that: "È assolutamente pacifico che la normativa di cui all'art. 615-*ter* c.p., presentandosi come un'estensione della protezione generalmente assicurata ad ogni forma di domicilio, ha inteso reprimere qualsiasi introduzione in un sistema informatico che avvenga contro la precisa volontà dell'avente diritto". A subsequent decision – G.I.P. Roma, 21 aprile 2000 – further clarified that: "Il legislatore, con l'introduzione della norma incriminatrice di cui all'art. 615-*ter* c.p., ha inteso tutelare non la privacy di qualsiasi domicilio informatico, ma soltanto quella dei sistemi protetti contro il pericolo di accesso da parte di persone non autorizzate. (…) Considerato che l'esistenza di mezzi efficaci di protezione costituisce elemento costitutivo della fattispecie incriminatrice di cui all'art. 615-*ter* c.p., deve dichiararsi il non luogo a procedere".

tralized, and expandable nature. Unlike physical locations, the digital network is not confined by tangible boundaries but exists as a dynamic and interconnected structure[47].

This conceptual distinction becomes particularly relevant when considering precautionary measures in the digital domain, such as virtual restraining orders, which impose restrictions on an individual's ability to access, communicate, or interact within specific online environments. In this context, the legal recognition of digital spaces as protected domains – analogous to physical domiciles – remains a crucial yet unresolved issue in many legal systems.

In light of these considerations, it becomes evident that the notion of a physical domicile cannot be straightforwardly transposed onto the digital sphere. Firstly, unlike a computer domicile, a physical domicile is not subject to the requirement of security measures. Under Article 614 c.p.[48], the right to the inviolability of one's home is not contingent upon the implementation of protective barriers, meaning that the victim is not responsible for equipping their home with security measures[49]. In contrast, the legal recognition of a computer domicile is intrinsically linked to the presence of security mechanisms, effectively placing a degree of responsibility on the user to safeguard their digital space. Unlike physical homes, the legal protection of the computer domicile is not generic; rather, it is conditioned upon the existence of security measures implemented by the system owner to protect the confidentiality of data, programs, or information. This requirement underscores the distinct nature of the computer domicile and confirms that it cannot be equated with its physical counterpart. However, once such protective measures are in place, the protection extends independently of the physical location where the data are stored (whether on a personal device, a corporate server, or a remote cloud infrastructure)[50]. The computer domicile should thus be understood as an autonomous legal asset, characterized by its intangible nature and the manifestation of the owner's will to exclude third parties through technological means, rather than by spatial or territorial boundaries.

In comparative perspective, the Spanish equivalent to Article 615-*ter* c.p. is Article 197-*bis* CP (Spanish Penal Code), which is located in Title X (Offenses Against Privacy, the Right to One's Own Image, and the Inviolability of the Home), Chapter I (Discovery and Disclosure of Secrets). This provision transposes Directive 2013/40/EU of August 12, concerning attacks against information systems and the interception of electronic data, provided that the intercepted data does not constitute personal communication[51].

Both the Spanish and Italian provisions addressing the unauthorized access to computer systems require the presence of a pre-existing "digital bar-

47. In this sense, an Italian criminal law sector considers that the limits and corporeality are merely incidental, not substantial, elements of the concept of place, so it aligns more with the idea of being a space potentially suitable for containing something (as would happen, for example, with air). With this conception in mind, it would be possible to consider the network as a "place". See, Signorato 2018.

48. Specifically, the criminal conduct of this offense consists of the intrusion of any person into another person's home, or another private residence, or its dependencies, against the express or tacit will of the person who has the right to exclude them, or having entered clandestinely or by means of deception.

49. At this point, the proposal put forward by Picotti, Flor and Salvatori regarding the placement of this type of offense (as well as others related to it) within a new, autonomous Section of the "Crimes Against Individual Liberty", under the title "On Crimes Against Privacy and Computer Security" (*Dei delitti contro la riservatezza e la sicurezza informatiche*), is particularly interesting. They also propose revising Article 615-*ter* of the Penal Code to remove, among other changes, the reference to the requirement that the computer system, or a part of it, must have security measures in place in order to be subject to criminal protection. See, Picotti–Flor–Salvatori 2021.

50. For example, an individual using their laptop in public still has the right to privacy regarding its content, protecting it from any public or private intrusion. See e, Trogu 2019.

51. In this regard, among the requirements of the Directive, it is called for a clear separation between cases of data disclosure that directly affect individuals' privacy and access to other data or information that may affect privacy but are not directly related to personal intimacy. In this way, accessing a personal contact list would not be the same as collecting data related to the software version used or the status of the entry ports to a system.

rier" (such as passwords or access credential) for virtual intrusion to be legally actionable[52]. This requirement stems from the assumption that the existence of protective measures against unauthorized access reflects the system owner's explicit intent to exclude third parties.

Within the Spanish framework, Article 197-*bis* CP specifies that the perpetrator must lack authorization to enter the system, thereby emphasizing the unlawfulness of intrusion beyond permitted access boundaries.

In the Italian context, the corresponding Article 615-*ter* c.p., criminalizes unauthorized access to computer or telematic systems. The jurisprudence of the Court of Cassation has progressively refined the interpretation of this provision, particularly regarding the scope of authorization and its functional limits. The prevailing view, firmly established by the *Sezioni Unite* in Judgment No. 41210 of 18 May 2017 (filed 8 September 2017), affirms that the offence may be committed not only by individuals who lack any formal authorization, but also by those who, while holding valid credentials, access or remain within a system for purposes alien to, or exceeding, the legitimate scope of their authorization, a phenomenon described as *sviamento di potere* ("abuse of authority" or "deviation of power").

The Court's reasoning is grounded in a functional and purpose-oriented interpretation of authorization. Access rights are valid only insofar as they serve the institutional or professional objectives for which they were granted. When an individual uses authorized credentials for private, competitive, or otherwise illegitimate purposes, the authorization loses its justificatory force, and the conduct constitutes "unauthorized access" within the meaning of Article 615-*ter*. The Court emphasized that the criminal provision protects not only the system owner's exclusive control but also the fiduciary integrity and internal trust that underpin the lawful use of digital credentials.

This interpretation extends criminal liability to situations where an employee or official, though possessing valid credentials, exploits them for purposes extraneous to their duties (for instance, accessing confidential corporate data to gain personal advantage or to cause harm).

This jurisprudential approach underscores that the mere possession of access credentials does not exclude criminal liability. The offence materializes whenever the authorized user accesses or remains within a system for reasons incompatible with the legitimate purposes of their authorization, thereby violating the protected interest in the confidentiality, security, and integrity of information systems.

However, unlike the Italian legal system, Spanish law does not recognize the autonomous concept of a "computer domicile". Furthermore, an equivalence between the physical and computer domicile – analogous to the Italian jurisprudential approach – would conflict with the case law of the Spanish Supreme Court regarding "virtual" intrusions into the domicile. A key reference in this regard is Supreme Court ruling 329/2016, dated April 20[53], which emphasizes that a domicile, as a constitutionally protected space, does not lose its legal status simply because curtains are left open or because the resident does not employ sufficient physical barriers to obstruct visibility from the outside. As Martín Ríos[54] argues, applying this reasoning to the computer domicile would mean that the mere absence of technical barriers preventing access to a device does not justify unauthorized access.

Such an approach reflects a broader understanding of information privacy in the digital age, grounded in the recognition that digital spaces, by their very nature, constitute extensions of the individual's private sphere. Even when accessed data does not immediately relate to personal privacy – such as traffic or location data – it may, when isolated or combined with other datasets, enable the reconstruction of an individual's private sphere, thereby infringing upon the same legal interests protected by traditional privacy provisions.

Accordingly, the absence of technological barriers should not diminish the protection afforded

52. This has even been acknowledged by the ruling of the Court of Cassation on October 27, 2004, which establishes that the crime of unauthorized access cannot be considered committed if the computer or telematics system to which the accused gains access is not objectively protected by security measures.

53. The well-know "sentencia de los prismáticos".

54. Martín Ríos 2017.

to digital environments. Just as the legal protection of the physical domicile does not depend on the presence of physical exclusionary measures (e.g., a locked door or closed curtains), digital spaces should enjoy equivalent safeguards given the quantity and sensitivity of information they contain. In other words, the absence of a password-protected login screen on a personal laptop should not justify unauthorized third-party access[55]. The legal protection of digital environments must therefore derive from their informational function rather than their technical configuration. The normative value of informational privacy – as a manifestation of personal autonomy and human dignity – demands equivalent protection in both physical and virtual domains. From a criminal policy perspective, this alignment is essential to ensure coherence between the material realities of cyberspace and the fundamental rights architecture of contemporary European criminal law.

Moreover, the evolving nature of digital spaces and the diverse functions that a single virtual environment can serve preclude rigid classifications of legal protections. For instance, a social media platform, such as Twitter, facilitates both public communication and private interactions. Within such an environment, users may not only have a general expectation of privacy but, in some cases, an enhanced expectation comparable to that associated with a physical home. This occurs when a user activates all available privacy settings, restricting access to their content to a select group. In such cases, unauthorized access to their digital space could constitute a significant violation of their legally protected privacy rights.

In this regard, both doctrine and jurisprudence of the Italian Court of Cassation[56] emphasize that a personal computer should not be regarded merely as a tool for processing and storing electronic documents. Instead, it represents an essential medium for cataloging, applying, and researching information (one through which individuals develop their professional, cultural, and intellectual capacities)[57]. Furthermore, the Court of Cassation has articulated a doctrinal interpretation concerning the expansion of the constitutional concept of domicile to encompass computer systems and virtual spaces. By adopting a teleological interpretation of the relevant legal provisions, the Court has asserted that the legislature intended to safeguard the "extension of the material domicile and the ideal space (including the physical location where digital data is stored) belonging to an individual, to which the right to privacy extends as a constitutionally protected right (Article 14 of the Constitution)". Consequently, the Court has recognized the concept of "computer domicile" as an additional manifestation of traditional domicile, grounded in the ius excludendi alios principle, regardless of

55. Specifically, according to Circular3/2017, of September 21Circular 3/2017, of September 21, it is not considered that the legal interest protected by Article 197-*bis* CP is the "computer domicile", nor that it directly attacks personal privacy. Instead, it is more about safeguarding "the security of information systems as a means of protecting the reserved privacy area from potential public knowledge". In this way, as highlighted in the Preamble of Organic Law 1/2015, the autonomous classification of this figure aims to establish a distinction between the cases referred to in Article 197 CP (related to the unauthorized access, seizure, or knowledge of data or information affecting personal privacy) and those in which, although there is illegal intrusion into third-party data or systems, personal data or privacy are not directly affected. However, even if there is no direct impact, as we mentioned earlier, computer data entered into a system, seemingly disconnected from a user's privacy, can, when examined as a whole, be highly revealing of the user's privacy, even leading to the creation of a fairly comprehensive profile of the individual. It is important to remember that this situation is referred to as the "mosaic theory".

56. Cuomo 2000; Aterno 2000. In case law, see Cass., Sez. VI, 4 ottobre 1999, n. 3067, and, more recently, Cass., Sez. Un., 27 ottobre 2011, n. 4694.

57. Signorato refers to the creation of a new sphere of protection for a new right, stemming from the development of new technologies. This would be a fundamentally dynamic right, not static, like the right to a computer domicile: the right to the inviolability of digital life (*diritto all'intangibilità della vita digitale*). However, this right differs from the right to self-determination over the use of personal data (*diritto all'autodeterminazione sull'uso di dati personali*), as the right to the inviolability of private life would not be limited to guaranteeing subjective protection restricted to personal data, but would extend to any data or activity inserted or developed within the realm of a computer system and the network. See, Signorato 2018.

the nature of the stored data, provided it pertains to an individual's intellectual or professional activities[58].

This expansion of the traditional notion of domicile to the "digital projection of the individual" aligns with the rationale underlying the "right to the integrity and privacy of information systems" recognized by the German Federal Constitutional Court. This right has emerged specifically to protect individuals from state access to their digital devices, particularly in cases involving government surveillance of entire information systems rather than merely individual communications or data storage activities[59].

Ultimately, the debate on "computer domicile" centers on whether materiality and physical boundaries are essential for recognizing a "place" subject to criminal law protection. This conceptualization is particularly relevant to the application of precautionary measures. In an online context, a restraining order – traditionally understood as a prohibition on approaching specific physical locations – could be adapted into a "virtual restraining order", restricting the accused from accessing designated digital spaces to prevent interaction with the victim. Notably, such an order would not be limited to direct communication but could also encompass shared virtual spaces where both individuals coexist within the same digital environment (despite thede absence of direct communication).

While restraining orders were initially designed to protect an individual's physical integrity by restricting access to certain locations, they are equally relevant in the digital realm, where psychological integrity can be compromised by an individual's virtual presence. This further justifies the legitimacy of implementing a virtual restraining order as a precautionary measure.

Although the Spanish legal framework does not explicitly recognize the concept of "computer domicile" as developed in Italian and German law, a related notion does exist: the "right to one's own virtual environment". This term was referenced in Supreme Court Judgment 342/2013, of April 17, and later reaffirmed in Judgment 786/2015, of December 4, although it has yet to receive formal legislative recognition. This "right to one's own virtual environment" could serve as a means of addressing the current fragmented regulatory landscape, in which protection against intrusions into electronic devices must be sought through separate legal provisions related to privacy rights (Article 18.1 CE), secrecy of communications (Article 18.3 CE), and data protection (Article 18.4 CE). Despite this fragmentation, the practical consequence remains the same: any measure involving interference with electronic devices or information systems requires prior judicial authorization[60].

This requirement would equally apply to a virtual restraining order. Indeed, enforcing such a restriction – limiting an individual's online interactions or access to specific digital spaces – may necessitate technological mechanisms to ensure compliance. Given the potential impact on fundamental rights and the need to uphold the principle of proportionality, judicial authorization would be indispensable. This requirement precludes law enforcement authorities or the Public Prosecutor's Office from imposing such measures without judicial oversight during the preliminary investigative phase. Moreover, in cases requiring access to an individual's digital devices or systems, the concept of "digital privacy" may serve as an enhanced dimension of general privacy protections. Since such access could involve highly sensitive information, express judicial authorization would always be required before proceeding with any measure affecting digital privacy rights[61].

Since the Spanish legal system does not explicitly recognize the concept of "computer domicile" as a legally protected interest, it has only recently begun to explores the possibility of extending the traditional concept of "place" from the physical

58. Domenicali 2018.

59. BVerG, February 27, 2008. Translation extracted from Venegoni–Giordano 2016.

60. Martín Ríos 2017.

61. As recognized in the aforementioned Constitutional Court ruling 173/2011 of November 7 and in Supreme Court ruling 786/2015 of December 4, the safeguarding of this right, like the inviolability of the home or the right to the secrecy of communications, is granted a higher level of protection than that afforded to privacy "in general".

to the virtual realm, particularly in response to the rise of cybercrime. Notably, Supreme Court ruling 547/2022, of June 2, considered the possibility of extending the concept of "place of the crime" to include social networks – and, by extension, the Internet – as a locus of criminal activity. According to the Court, within the scope of Article 48 of the Spanish Penal Code, the prohibition on accessing certain locations could be interpreted to encompass digital spaces of interaction and communication where offenses were committed. However, the dissenting opinion in this ruling warns that this analogical interpretation risks overstepping the boundaries set by the principle of legality in criminal law, particularly concerning the legitimacy of penalties.

This concern highlights the distinction between restricting access to physical and virtual spaces. While prohibiting entry into a physical location primarily limits an individual's freedom of movement (albeit in a limited manner), restricting access to a social network would directly impact freedom of expression, and, arguably, the right to Internet access. Consequently, repurposing an existing legal measure originally designed for physical spaces to restrict access to online spaces could constitute a "label fraud"[62] of legal concepts. This would distort the true nature of the measure, concealing under one label what is, in reality, a different type of restriction: a limitation on freedom of expression and Internet access.

Given these considerations, it is imperative to establish a distinct precautionary measure – separate from traditional restraining orders – specifically tailored to the digital sphere. This would prevent "label fraud" and ensure that such measures are properly framed within the principles of legality and proportionality.

From this perspective, we argue that the proposed virtual restraining order could be accommodated within the Spanish legal framework. This measure could take the form of a temporary prohibition limited to the digital space where the offense was committed, such as a specific social network, forum, or platform. In particularly severe cases (where, for instance, the offense was committed across multiple platforms or websites, and the harm inflicted upon the victims is significant) broader restrictions, such as a general prohibition on Internet access or a ban on contracting with Internet Service Providers, could be considered. The following sections will further explore these potential applications.

4.2.2. Prerequisites for the adoption of the virtual restraining order: special reference to the principle of proportionality

Due to the profound implications that cyber-precautionary measures – such as the proposed virtual restraining order – may have for fundamental rights (including freedom of expression, Internet access, informational privacy, and even the emerging right to one's "digital environment"), the principle of proportionality assumes a central and indispensable role in ensuring their constitutional legitimacy and practical effectiveness. It functions not merely as a balancing mechanism but as the normative threshold distinguishing legitimate precautionary intervention from disproportionate encroachment on digital freedoms.

Since Internet access plays a crucial role in individuals' personal and professional development, as well as their integration into the digital sphere, a preliminary balancing test tailored to the specific circumstances of each case is indispensable[63].

Therefore, the application of a virtual restraining order must be assessed in relation to the protection of legally recognized interests, provided that these aims withstand a proportionality test demonstrating the necessity of the measure. This principle serves as an essential analytical tool for evaluating the rational connection between the means employed and the objectives pursued – namely, preventing recidivism and further harm to victims – while seeking to resolve conflicts between competing rights or interests. Ultimately, the suitability, necessity, and proportionality in the strict sense of

62. The term "label fraud" (*Etikettenschwindel*), used almost a century ago by Kohlrausch, refers to the attempt to assign the legal regime of one institution to another simply by labeling it with the name of the former. In this regard, our Constitutional Court, in its ruling 239/1988, already argued that the *nomen iuris* of an institution cannot be a determining factor. See, Puente Rodríguez 2019.

63. Pollicino, 2023.

the measure must be assessed on a case-by-case basis[64], precluding any automatic application.

As established in Article 52(1) of the Charter of Fundamental Rights of the European Union (CFREU) [65], any limitation on the exercise of fundamental rights – such as privacy (Article 7), data protection (Article 8), and freedom of expression (Article 11) – must be provided for by law, respect the essence of those rights, and, subject to the principle of proportionality, be necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others. This principle thus serves as the analytical framework for judicial scrutiny of cyber-precautionary measures.

The Court of Justice of the European Union (CJEU) has progressively delineated the contours of proportionality in a series of landmark decisions concerning data retention, surveillance, and investigatory powers. In *Digital Rights Ireland* (Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238), the Court invalidated the Data Retention Directive for disproportionately interfering with the rights to privacy and data protection, stressing that general and indiscriminate retention of electronic communications data exceeds what is necessary in a democratic society. The CJEU reaffirmed and deepened this approach in *Tele2 Sverige AB and Watson* (Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970), holding that only targeted and temporally limited retention, based on objective criteria and subject to prior independent review, can satisfy the proportionality requirement.

Similarly, in *La Quadrature du Net* (Joined Cases C-511/18, C-512/18, and C-520/18, 6 October 2020, ECLI:EU:C:2020:791), the CJEU reiterated the centrality of the principle of proportionality in the context of data retention measures affecting fundamental rights. The Court emphasized that any derogation from the protection of personal data must be strictly necessary and proportionate to the legitimate objectives pursued. It held that national legislation permitting the general and indiscriminate retention of traffic and location data for the purposes of combating crime and safeguarding public security exceeds the limits of what is strictly necessary and cannot be justified within a democratic society. The CJEU further clarified that only measures aimed at combating serious crime, preventing serious threats to public security, and safeguarding national security are capable of justifying such serious interference. Furthermore, the Court emphasized that retention must be limited in scope and duration, both in terms of the categories of data affected and the period of storage, and must be governed by clear, precise, and foreseeable rules providing effective safeguards against abuse. This reasoning encapsulates the CJEU's broader digital proportionality doctrine: the more intrusive the measure, the more stringent the justification required. The judgment thus consolidates a structured proportionality standard which national authorities must satisfy when implementing precautionary or investigative powers that restrict digital freedoms.

The European Court of Human Rights (ECtHR) has adopted a complementary stance. In *Ahmet Yildirim v. Turkey* (2012) and *Cengiz and Others v. Turkey* (2015), it condemned broad Internet blocking orders as disproportionate under Article 10 ECHR, emphasizing that such measures must pursue a legitimate aim, rest on clear legal grounds, and preserve the essence of freedom of expression and information. The same reasoning applies to precautionary restrictions imposed in the digital environment: they must be targeted, necessary, and reversible. Likewise, in *Roman Zakharov v. Russia* (App. No. 47143/06, Judgment of 4 December 2015) and *Big Brother Watch and Others v. the United Kingdom* (App. Nos. 58170/13, 62322/14, and 24960/15, Judgment of 25 May 2021), the ECtHR emphasized that surveillance and data

64. This is known as the "German test". The position of Spanish Constitutional Court regarding the applicability of the principle of proportionality can be observed in ruling 11/1981, FJ 7.

65. This principle of proportionality is also reflected in Article 8 of the European Convention on Human Rights, which, under the heading "Right to respect for private and family life", states that there shall be no interference with this right by public authorities unless "such interference is in accordance with the law and constitutes a measure that, in a democratic society, is necessary for national security, public safety, the economic well-being of the country, the defense of order and the prevention of criminal offenses, the protection of health or morals, or the protection of the rights and freedoms of others".

interception measures must be "necessary in a democratic society," subject to rigorous *ex ante* judicial authorization, foreseeability, and end-to-end proportionality assessment.

The convergence between the CJEU and ECtHR jurisprudence illustrates that proportionality functions as a structural and cross-systematic principle ensuring that the expansion of digital precautionary powers remain compatible with fundamental rights. In the context of cyber-precautionary measures such as the virtual restraining order, this convergence provides the normative compass: restrictions must be individualized, temporary, and judicially supervised, ensuring that the protection of victims does not erode the foundational liberties inherent to the digital public sphere.

This jurisprudential alignment finds strong resonance in European legal scholarship. Herlin-Karnell[66] argues that proportionality in EU criminal law operates not merely as a balancing tool, but as a constitutional compass preventing the creeping normalization of intrusive technologies under the guise of efficiency. Ashworth and Zedner[67] in *Preventive Justice* conceptualize proportionality as the key criterion distinguishing legitimate precautionary intervention from preventive overreach. In Italy, as noted by Torre[68], digital investigations embody in their most acute form the traditional tension between the protection of individual rights and the demands of social defense. In this context, the solution must rest on a rigorous and structured application of the principle of proportionality, ensuring a careful balancing of the competing legal interests at stake. The proportionality principle serves not only as a limit to the State's coercive powers but also as a structural guarantee of their legitimacy. By requiring a reasoned evaluation of suitability, necessity, and proportionality *stricto sensu*, it transforms judicial discretion into a transparent process of normative justification.

The Spanish Constitutional Court has similarly recognized proportionality as an essential condition of legitimacy for any measure restricting rights. In STC 292/2000 and STC 49/1999, the Court held that restrictions must be (a) suitable to achieve their purpose, (b) necessary in the absence of less restrictive alternatives, and (c) proportionate *stricto sensu*, ensuring that the sacrifice of individual rights does not exceed the benefits for the public interest. These standards apply fully to cyber-precautionary measures, which by their very nature intersect with rights to communication and information.

On the basis of the foregoing, a virtual restraining order should not, as a general rule, entail a blanket prohibition on Internet access. Rather, any restriction must be narrowly tailored to the specific circumstances of the case, such as the severity of the offense, the risk of reoffending, the potential harm to victims or other legal interests, and the technological proficiency of the investigated individual. Accordingly, in certain situations, a targeted restriction – such as blocking access to the specific website, platform, or application through which the unlawful conduct occurred – may suffice. In more severe cases (e.g., online child exploitation, gender-based violence, or systematic cyberstalking), technically enhanced measures, including the installation or execution of judicially approved software, may be required to prevent the investigated individual from re-entering the victim's digital environment. Only in cases of exceptional gravity could a temporary, general prohibition on Internet access, or a ban on entering into contracts with Internet Service Providers, meet the proportionality threshold.

It is axiomatic that any limitation of fundamental rights must have a clear legal basis. Legislation must precisely define the conditions, scope, and duration of such measures. Judicial authorization and oversight are indispensable, both *ex ante* – to approve and delimit the measure – and *ex post* – to monitor its implementation and termination. Such measures cannot be authorized by an administrative body, let alone by ISPs or digital platforms. To ensure compliance with the principle of proportionality, any judicial order authorizing a virtual restraining measure must specify:

- the devices, systems, or digital environments affected or parts thereof;
- the extent and technical modalities of the restriction;

66. Herlin-Karnell 2012.

67. Ashworth–Zedner 2014.

68. Torre 2019.

– the software or monitoring tools authorized;
– the duration, strictly limited to what is necessary.

Additionally, if there is evidence that the investigated individual has access to other devices that could undermine the effectiveness of the order, law enforcement authorities must notify the judge, who may authorize an extension of the measure's scope to ensure its effectiveness.

Regarding duration, and in alignment with the requirements established for other existing cyber-precautionary measures, the order must be strictly limited to the minimum time necessary to fulfill its protective function[69]. Naturally, the measure must be lifted as soon as the circumstances that initially justified its adoption cease to exist, preserving the proportional equilibrium between public protection and individual freedom.

Within this framework, the virtual restraining order exemplifies a measure that – while restrictive of certain digital freedoms – can remain constitutionally legitimate when applied under stringent judicial oversight, subject to temporal limits, and demonstrably necessary to prevent reoffending and protect victims from renewed harm in online environments.

The cooperation of Internet Service Providers and digital intermediaries is crucial to enforce such measures effectively. These entities must be legally bound by a duty of cooperation as well as an obligation of confidentiality concerning such activities, ensuring that the execution of judicial orders in the digital sphere is both effective and rights-compliant. In the event of non-compliance, they could be subject to criminal liability for disobedience of a judicial order[70]. However, as Starr[71] aptly observes, the delegation of enforcement functions to private digital actors – when performed negligently or without adequate legal safeguards –, risks turns them into *de facto* agents of state authority, thereby blurring the constitutional boundaries between public accountability and private discretion. Such a shift would undermine the principle of legality and erode the transparency that judicial control is designed to guarantee. Consequently, any cooperative framework must be narrowly defined, normatively grounded, and subject to continuous judicial oversight to avoid the privatization of coercive functions within cyberspace.

This participatory model aligns with the EU's Digital Services Act (Regulation 2022/2065), which emphasizes judicial oversight, due process, and accountability in the moderation of online content. By analogy, cooperation in enforcing this online restriction order must likewise be governed by transparent, rights-based standards.

In this regard, proposals such as Bajovic's concept of a "cyber-deportation," whereby a cyberspace police force could impose temporary Internet bans, raise profound constitutional concerns. According to Bajovic, since such a measure would not constitute a criminal sanction, the debate surrounding the right to a fair trial would not be applicable. She argues that the presumption of innocence remains intact, given the preventive, temporary, and non-punitive nature of the restriction. Under this framework, judicial safeguards would be available at a later stage before the national court, drawing an analogy with pretrial detention in traditional criminal proceedings, which can serve the same purpose of preventing recidivism[72].

While this theoretical approach is undoubtedly thought-provoking, even acknowledging the deterrent effect she defends, it presents significant shortcomings. First, it fails to specify how such an Internet access ban would be technically enforced or what its practical implications would be. Second, it grants discretionary authority to a cyberspace police force, despite the fact that, as previously noted, any measure temporarily restricting access to the Internet or specific online content inherently affects fundamental rights. As such, these restrictions cannot be left to extrajudicial powers, as their imposition must strictly adhere to the principle of proportionality on a case-by-case basis and must always require judicial intervention.

69. In this case, it is concretized in preventing recidivism and the attack on new legal assets of the victim.
70. Application, *mutatis mutandis*, of the provisions of Article 588-*ter* e) LECrim concerning the obligation of ISPs to cooperate.
71. Starr 2025.
72. Bajovic 2017.

In contrast, the virtual restraining order proposed here preserves judicial centrality. By requiring court approval, defining the technological implementation, and ensuring procedural safeguards, it reconciles efficiency and legality while maintaining coherence with EU and ECHR proportionality standards.

In sum, the principle of proportionality serves as the constitutional compass for cyber-precautionary measures, ensuring that preventive protection does not devolve into digital repression. Only through this equilibrium can the criminal justice system uphold its dual mission in the digital era: to protect victims and society while safeguarding individual rights against excessive or arbitrary interference.

4.3. Implementation of the virtual restraining order

Preventing an individual from accessing the Internet entirely is an almost impossible task, given the multitude of devices available for such access. Similarly, it is equally unfeasible to prevent someone from committing any criminal act unless they are held in a maximum-security prison under constant surveillance. As we know, suspending an individual's driver's license does not physically prevent them from operating a vehicle (whether by using one belonging to a family member or even a stolen one). The same applies to firearm prohibitions, as weapons can still be acquired on the black market. These examples illustrate the inherent difficulty of ensuring that a legal measure or sanction alone completely prevents an individual from engaging in a specific conduct. Therefore, Internet restrictions do not guarantee total compliance. Instead, the objective is to increase the difficulty of engaging in illicit activity by depriving individuals of the means to do so, while ensuring that any breach of the restriction carries a specific legal sanction, which serves as the true deterrent.

Accordingly, the virtual restraining order we propose does not aim to completely prevent Internet access or specific online content but rather to impose targeted restrictions in cases where such a precautionary measure is justified[73].

At this juncture, the possibility of implementing tailored blacklists (*ad hoc*) could be considered. These would consist of a list of websites that a specific individual is prohibited from accessing. Such personalized blacklists would be transmitted to the individual's ISP, which would disable access through technical means. To ensure compliance with the principle of proportionality, victims could be consulted regarding which social networks or online platforms they use, allowing for a precise and dynamic application of the restraining order. These lists would be periodically updated, with online sites being added or removed based on the evolution of the case and advancements in technology.

From an operational standpoint, two main scenarios could be considered for implementing this precautionary virtual restraining order:

1) Identifying the individual accessing the Internet, thereby allowing a specific online connection to be attributed to a particular person. This would require the establishment of a digital identity system.
2) Restricting Internet access on a particular electronic device associated with the investigated individual, without the capability to confirm whether that individual is indeed the one using the device at the time of the connection.

Both approaches require further legal and technical development to ensure their feasibility and compliance with fundamental rights.

4.3.1. Digital identity system

In the context of digital security and online accountability, the implementation of digital identity systems could be considered as a mean to directly associate a specific individual to a given IP address. Such a system would enable a direct association between an individual and their online activity, thereby allowing for targeted restrictions on Internet access during the enforcement period of a precautionary measure. Through this mechanism, a specific individual could be prevented from accessing the virtual environment for the duration of the imposed sanction.

Regarding digital identification on the Internet, a noteworthy initiative is "Proof of Humanity" (PoH), a system designed to enhance security in a decentralized digital ecosystem. PoH is a social

73. In the terms outlined in the previous section.

identity verification system built on Ethereum[74], aimed at enabling individuals to access various applications that require resistance to Sybil attacks[75] for large-scale implementation. The system integrates webs of trust, reverse Turing tests, and dispute resolution mechanisms to create a Sybil-resistant registry of verified human users. Registration requires multiple verification steps, including the creation of a video with a spoken statement, the linkage of an Ethereum address to a clearly identifiable profile, and endorsement by an already verified user. Each individual can only register one account.

PoH-verified accounts could serve multiple purposes, including functioning as universal login methods and integrating with other identity systems to strengthen Sybil resistance in user profiles[76]. However, this system raises concerns regarding online anonymity, a fundamental characteristic of the Internet. Currently, PoH-stored identities are not anonymous, prompting efforts to develop privacy-preserving, Sybil-resistant digital identities. Proposed solutions include Traceable Ring Signatures and zero-knowledge proof mechanisms[77], which would allow individuals to verify their humanity without disclosing their identity[78].

Similarly, Tools for Humanity Corporation (TFH), as part of the Worldcoin project, has developed World ID[79], a digital identity system designed to safeguard user's privacy. World ID verifies an individual's humanity through an iris scan, generating a unique numerical code intended to preserve user anonymity. This digital identity functions as a "digital passport" or "identity wallet" stored on the user's phone, which can be used anonymously to verify that the individual is real and unique. The system operates via The Orb, a biometric device that scans iris patterns within seconds, creating a unique digital record of human identity[80].

Despite their innovative approach, both Proof of Humanity and World ID raise critical concerns regarding personal data protection. Fundamental questions remain unanswered: How are these biometric data processed? Who has access to them? What are the risks of data breaches, theft, or unauthorized access? If these concerns are not adequately addressed with robust safeguards, these systems could lead to significant violations of privacy rights and potential abuses of personal data.

From a doctrinal standpoint, Bajovic has explored the feasibility of biometric authentication replacing traditional username-password methods. She argues that biometric markers, such as fingerprints, could serve as digital passports for Internet access, drawing a parallel to state-controlled border security mechanisms. In her view, regulating movement in cyberspace through biometric authentication could be a necessary response to rising cybercrime rates. This proposal suggests the

74. According to its official page, EthereumEthereum is a network of computers worldwide that follow a set of rules known as the Ethereum protocol and it serves as the foundation for communities, applications, organizations, and digital assets that anyone can build and use.

75. A Sybil attack is a security threat to a P2P network that involves the control of multiple fake identities through a single device, known as a node. The scheme is similar to creating multiple accounts on a social network by the same user. In this way, a single attacker can run more than one node (IP addresses or user accounts) simultaneously on the Internet. During a Sybil attack, each fake identity appears to be real, as if they were legitimate nodes operated by different users.

76. Likewise, the creation of PoH could ensure, if necessary, that the creator of a digital property is human, rather than an AI, serving as an important complement to blockchain and positively influencing its transparency and fairness by introducing bot blocking in the chain to provide a decentralized solution for decentralized networks.

77. Also known as Zero Knowledge Protocol (ZKP).

78. For example, it could be used in the context of KYC (Know Your Client), allowing privacy to be preserved by providing a zero-knowledge proof that demonstrates one is a citizen of a specific country or over a certain age without revealing their identity.

79. Company behind ChatGPT.

80. The procedure involves downloading the Worldcoin app, then registering with a phone number, followed by receiving a QR code. Next, at one of the locations where the orbs are placed – a silver device in the shape of a sphere – an ocular scan is performed and the verification is generated.

mandatory implementation of biometric security systems to control online access.

Although this idea presents intriguing possibilities – such as linking a biometric marker[81] to a judicially imposed virtual restraining order to restrict an individual's access to certain online spaces – there are substantial legal and ethical obstacles to the large-scale implementation of biometric identification systems. These challenges extend beyond technological feasibility and raise fundamental concerns about freedom of expression, privacy, and online anonymity[82].

Particularly, the compatibility of biometric access control systems with the Regulation on Artificial Intelligence (AI Act), recently adopted by the European Union, has been the subject of evolving discussions. The initial draft of the AI Act distinguished between real-time and non-real-time biometric identification systems. Real-time systems process biometric data instantaneously or with minimal delay, whereas non-real-time systems collect and analyze biometric data after a significant delay.

Given its operational model, biometric authentication for Internet access would likely fall under real-time biometric identification, where fingerprints or iris scans are instantly analyzed to grant access. Under the AI Act's original provisions, such systems were classified as high-risk due to their potential to infringe upon users' privacy, limit their personal freedoms online, and create a sense of constant surveillance, ultimately discouraging free expression and online activity[83].

However, in its first reading on March 13, 2024[84], the European Parliament introduced amendments excluding certain biometric verification systems from the category of real-time biometric identification. Specifically, the final version of the AI Act, adopted on May 21, 2024, and published on July 12, 2024[85], explicitly exempts AI-driven biometric verification systems used solely for authentication purposes, such as verifying an individual's identity for accessing Internet services, unlocking devices, or securing facilities. Additionally, Annex III of the AI Act maintains the classification of remote biometric identification systems as high-risk but excludes verification systems used exclusively to

81. Whether it is a fingerprint or the iris.

82. Faced with the idea of feeling identified and monitored, users may begin to self-censor. This is what we could call "digital panopticism" (in an analogous reference to Bentham's panopticon). Indeed, if an individual feels surveilled (even when they are not), they will act as if they were.

83. From another perspective, we could also argue that, while it is true that there must be freedom to navigate the Internet, this must occur within the limits of what is socially and legally acceptable and permissible. Users should be able to feel free to act in the online world as they wish and express themselves in the way they deem appropriate, as long as they do not infringe upon the freedom of others. However, at the same time, they should have the fear of being discovered if they engage in online activities that violate internationally protected legal rights (since, as we have already pointed out, speaking in virtual terms simply based on state boundaries is an abstraction, just as it is in the physical world). However, we currently lack mechanisms that allow us to strike a balance between a sense of online freedom for users that does not restrict their online actions, and the necessary mechanisms to identify an internet user when investigating serious crimes. Therefore, given the palpable risk of infringing upon users' fundamental rights, we believe it is more prudent, for now, to adopt a position that favors the protection of online personal freedom, privacy, and other fundamental rights on the Internet.

84. Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative acts- Outcome of the European Parliament's first readingProposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative acts - Outcome of the European Parliament's first reading (Strasbourg, 11 to 14 March 2024).

85. Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, establishing harmonized rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, establishing harmonized rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1, published in the Official Journal of the European Union (OJEU) No. 1689, on July 12, 2024.

confirm an individual's identity (a carve-out based on the presumption that such systems pose a lesser threat to fundamental rights compared to mass biometric surveillance).

This regulatory clarification could accommodate Bajovic's biometric passport proposal, as it allows biometric markers to function as digital identity credentials.

However, from our point of view, biometric data collection and processing inherently involve handling highly sensitive personal information. These data are inextricably linked to the potential infringement of fundamental rights, particularly those related to privacy and personal integrity. The European Parliament, in its first reading position, has explicitly recognized that biometric information constitutes a special category of sensitive personal data and has acknowledged the intrusive nature of biometric identification systems for the individuals subjected to them. Consequently, even when biometric data are collected exclusively for legitimate purposes, their processing must be subject to robust and sufficient safeguards to prevent abuses stemming from improper management or storage.

The legal compatibility of biometric data collection with existing regulatory frameworks remains a complex and contentious issue. The final version of the AI Act could potentially conflict with key regulatory instruments, including Article 9.1 of the General Data Protection Regulation (GDPR), Article 10.1 of Regulation 2018/1725, and Article 10 of Directive 2016/680. These legal frameworks impose a general prohibition on the processing of biometric data aimed at uniquely identifying a natural person, allowing exceptions only under specific conditions. Among these, the sole applicable exception in this context would be the explicit and informed consent of the data subject. However, a fundamental question arises: to what extent can users fully comprehend the implications of their consent, particularly in relation to the surveillance risks it entails? It is imperative to establish mechanisms that ensure not only the effective collection of consent but also the provision of comprehensive information regarding the impact of biometric data processing on fundamental rights.

Beyond these legal considerations, if biometric authentication systems were to become a mandatory prerequisite for Internet access, the notion of freely given consent would be rendered highly questionable. In the current digital landscape, Internet access can no longer be considered an optional resource but rather an essential element of social and economic interaction. Indeed, as has been previously established in legal and academic discourse, Internet access has been recognized as a fundamental right in light of the pervasive and continuous nature of digital connectivity. Under these conditions, framing the provision of biometric data as a voluntary act would be a legal fiction, as the alternative – exclusion from digital life – is neither feasible nor proportionate.

Finally, any regulatory framework governing biometric data processing must aligned with fundamental procedural safeguards, including those enshrined in the Universal Declaration of Human Rights, the European Convention on Human Rights, and other relevant international and domestic legal instruments. To prevent emerging technologies from undermining rights originally designed for the physical world, classical procedural mechanisms – such as precautionary measures – must be adapted and reinterpreted within the digital domain. This recalibration is not merely advisable but an urgent necessity in the contemporary legal landscape.

4.3.2. *Restriction of network access for devices belonging to the investigated individual*

The establishment of a digital identity as a prerequisite for accessing the Internet – particularly when biometric identification methods are employed – poses significant challenges in terms of compliance with existing regulations on personal data protection, individual freedom, and the right to privacy. The primary concern arises from the erosion of online anonymity, a fundamental element of digital privacy. Given these legal and ethical constraints, the most immediate and practical approach to implementing a virtual restraining order as a precautionary measure would be to target the electronic devices linked to the investigated individual through which Internet access is sought[86].

86. However, it is clear that this can be more easily manipulated to bypass the prohibition or restriction on access, unlike biometric data, which cannot be tampered with.

In this context, it would be worth considering the requirement for the investigated individual to compile an inventory of electronic devices, a process in which ISPs with whom the individual has contracted network access services could play an active role. This inventory would serve as the basis for enforcing the virtual restraining order, allowing for the implementation of necessary technical modifications or software installations to restrict online access.

The proposed measure aims to temporarily restrict the ability of the investigated individual to access specific digital environments or online platforms through their personal devices. Its purpose is twofold: to prevent the continuation or repetition of unlawful online behavior and to ensure the effectiveness of ongoing investigations by limiting the suspect's capacity to interfere with digital evidence or victims.

In its technical implementation, the measure should rely on a hybrid enforcement model combining two complementary mechanisms: a cooperation framework with ISPs and, where legally and technically feasible, the use of access-control software installed on the individual's devices under judicial authorization. This dual structure ensures both proportionality and technical reliability.

Under the first component, collaboration with ISPs would allow the execution of network-level restrictions. ISPs could be required to block the investigated individual's access to specific domains, IP addresses, or platforms identified by judicial order. This approach guarantees that the restriction is implemented externally, at the level of network routing or domain resolution, without requiring intrusive monitoring of user data or communications content.

Such blocking may also extend to MAC (Media Access Control) addresses assigned to the investigated individual's devices, preventing connection to particular servers or online resources[87]. Nevertheless, these technical mechanisms present inherent limitations: both IP and MAC addresses can be easily obfuscated or spoofed with minimal expertise. For instance, an individual can employ a Virtual Private Network (VPN) to mask their real IP address by routing traffic through a remote server, or use MAC address spoofing to alter their device's network identity temporarily. These techniques, while legitimate for privacy purposes, are also routinely exploited by offenders to evade detection and bypass network-level access restrictions.

The second component – local access-control software – would apply in situations where ISP collaboration may prove insufficient. This occurs particularly when the investigated individual employs anonymization tools or alternative connection channels that operate beyond the effective reach of Internet Service Providers. For instance, if the individual connects to the Internet through public Wi-Fi networks, mobile hotspots, or virtual private networks that encrypt traffic and reroute it through foreign servers, ISP-based blocking orders issued within national jurisdiction may become ineffective. In such cases, a court-authorized software application could be installed on the individual's device(s) to enforce restrictions at the system level. The software would not intercept communications but would prevent connection attempts to specific sites, services, or applications, even when the device connects through networks not controlled by the designated ISP, thereby ensuring compliance with judicially mandated prohibitions. This solution should be subject to independent oversight to guarantee transparency, data minimization, and respect for fundamental rights.

Regardless of the enforcement mechanism adopted, the principle of proportionality must guide judicial decision-making. The measure should remain temporary, targeted, and necessary, limited to preventing access to online environments directly related to the alleged criminal activity (for example, platforms hosting illicit material or enabling further victimization). The choice between network-level blocking and device-level restriction – or a combined approach – should depend on technical feasibility, the nature of the investigated offence, and the degree of judicial control required.

87. It is not always easy to link a specific IP address, VPN, or MAC address to a particular person. Consequently, a direct connection between the owner of the IP address and the individual who committed the offense cannot be made. For instance, access credentials may have been stolen. Therefore, the fact that a person owns a line with a specific IP address does not constitute necessary and sufficient evidence to hold them accountable, unless there is other evidence pointing in that direction (Spanish Supreme Court, ruling 987/2012, December 3).

To reinforce compliance, these measures could also include a temporary prohibition on entering into new contracts with ISPs or purchasing additional Internet-enabled devices, except under judicially authorized circumstances. In such cases, appropriate safeguards must be established to ensure that any newly acquired device conforms to the existing access restrictions.

By adopting a calibrated hybrid model the combines ISP cooperation with judicially supervised technical safeguards, the proposed restriction of network access achieves coherence with the broader concept of cyber-precautionary measures. It is not designed to suppress a person's general access to the Internet, but to restrict digital interaction within specific illicit contexts, thereby aligning with the overarching objectives of criminal procedure in the digital era: preserving evidence integrity, preventing reoffending, and protecting victims from ongoing harm.

5. Conclusions

The evolution of criminal activity in cyberspace has challenged the foundations of traditional criminal procedure, revealing the inadequacy of precautionary mechanisms designed for an analogue world. The dematerialization of criminal conduct, the volatility of digital evidence, and the deterritorialized nature of online interactions demand a redefinition of precautionary action. Within this new paradigm, cyber-precautionary measures emerge as an indispensable legal instrument to ensure both the preservation of digital evidence and the protection of victims from ongoing harm in the digital environment.

The analysis developed throughout this study demonstrates that these measures possess a dual legal and functional nature. On the one hand, they serve an evidentiary function, aimed at preventing the alteration or destruction of digital content relevant to the proceedings. On the other, they fulfil a preventive and protective function, designed to interrupt the circulation of unlawful material and to safeguard victims from revictimization or renewed exposure. This duality reflects a necessary evolution of precautionary law toward a model that addresses not only the risks of procedural inefficiency but also the human and social consequences of cybercrime.

Nevertheless, the effectiveness of cyber-precautionary measures depends on the existence of a robust legal and technical infrastructure. National legal systems must articulate clear procedural guarantees, ensuring judicial control, transparency, and the protection of privacy and due process. At the same time, international cooperation remains essential, given the transnational nature of cybercrime and the global architecture of the Internet. Without coordinated mechanisms for enforcement and information exchange, the reach of national precautionary measures risks remaining merely symbolic.

The fight against cybercrime requires a precautionary paradigm attuned to the digital age: one that is technologically informed, normatively coherent, and procedurally fair. Cyber-precautionary measures, properly conceived and regulated, can bridge the gap between the law's traditional tools and the realities of cyberspace. They do not seek to expand punitive power but to ensure the effectiveness, proportionality, and humanity of criminal justice in a context where harm can spread at the speed of data.

The proposed "virtual restraining order" illustrates how precautionary law can evolve to meet the demands of a society increasingly shaped by technology, while maintaining fidelity to the fundamental principles of legality, proportionality and rights protection. However, the implementation of virtual restraining orders as a precautionary tool in cybercrime investigations presents both technical and legal challenges that must be carefully balanced to ensure effectiveness without disproportionately infringing upon fundamental rights. The proposed strategies offer viable solutions for limiting an investigated individual's online activity. However, their practical enforcement is constrained by the ease with which technologically adept individuals can circumvent them, particularly through techniques such as VPN usage or MAC address spoofing.

From a legal perspective, any measure restricting digital access must comply with overarching principles of proportionality, necessity, and legality. The erosion of online anonymity, inherent in some of these measures, raises critical concerns regarding personal data protection, individual freedom, and the right to privacy. Thus, a case-by-case judicial assessment is imperative, considering the

severity of the alleged cybercrime, the technological expertise of the investigated individual, and the potential impact of the restriction on their rights.

Additionally, the role of ISPs as key facilitators in the enforcement of these measures cannot be overlooked. Their cooperation in identifying, monitoring, and restricting access to specific devices is essential, yet it must be framed within a clear legal mandate to avoid excessive delegation of law enforcement powers to private entities.

Bearing in mind these complexities, a hybrid approach – combining technical restrictions with judicial oversight and regular re-evaluation of the necessity of the imposed measures – emerges as the most balanced solution. Furthermore, any regulatory framework governing such restrictions must remain adaptable to evolving technological advancements, ensuring that legal safeguards remain robust against emerging circumvention techniques.

Ultimately, while the virtual restraining order represents a promising avenue for addressing cybercriminal activities, their implementation must be meticulously calibrated to safeguard fundamental rights while upholding the legitimate interests of criminal investigations. Only through a nuanced, legally sound, and technologically informed approach can such measures achieve their intended purpose without compromising the broader principles of justice and due process.

Bibliographic references

I.J. Acata Águila (2011), *Internet, un derecho humano de cuarta generaciónInternet, un derecho humano de cuarta generación*, in "Misión Jurídica", vol. 4, 2011, n. 4

J.R Agustina Sanllehí, I. Montiel Juan, M. Gámez-Guadix (2020), *Cibercriminología y victimización online*, Síntesis, Madrid, 2020

R. Alexy (2002), *A Theory of Constitutional Rights*, Oxford University Press, 2002

T. Álvarez Robles (2024), *El Derecho de acceso a Internet. Especial referencial al constitucionalismo español*, Editorial Tirant Lo Blanch, 2024

T. Álvarez Robles (2022), *Las garantías de los derechos fundamentales en y desde la red: el contexto español*, in "Revista Chilena de Derecho y Tecnología", vol. 11, 2022, n. 1

A. Ashworth, L. Zedner (2014), *Preventive Justice*, Oxford University Press, 2014

Z. Aslam, J. Kaaniru, D. Abiero (2025), *Recognising Access to the Internet as a Fundamental Right: Political, Socio-economic, and Legal Perspectives,* Strathmore University, 2025

S. Aterno (2000), *Sull'accesso abusivo a un sistema informatico o telematico*, in "Cassazione Penale", 2000

V. Bajovic (2017), *Criminal Proceedings in Cyberspace: The Challenge of Digital Era*, in E. Viano (ed.) "Cybercrimen, Origanized Crimen, and Societal Responses", Springer, Cham, 2017

A. Bettiga (2020), *La tutela delle vittime di reati informatici*, in "Rivista italiana di diritto e procedura penale", 2020

J. Bustamante Donas (2010), *La cuarta generación de derechos humanos en las redes digitales*, in "Revista TELOS (Revista de Pensamiento, Sociedad y Tecnología)", 2010

J. Bustamante Donas (2001), *Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica*, in "Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación", 2001

E.J. Cova Fernández (2022), *Derechos Humanos y Derechos Digitales en la Sociedad de la Información*, in "Revista Derechos Humanos y Educación", 2022, n. 6

L. Cuomo (2000), *La tutela penale del domicilio informatico*, in "Cassazione penale", 2000

C. Domenicali (2018), *Tutela della persona negli spazi virtuali: la strada del "domicilio informatico"*, in "federalismi.it", 28 marzo 2018

T.E. Frosini (2011), *Il diritto costituzionale di acceso ad Internet*, in "Rivista AIC", 2011, n. 1

P. García Mexía (2018), *El derecho de acceso a Internet*, in T. De la Cuadra Salcedo, J.L. Piñar Mañas, (dirs.), "Sociedad digital y Derecho", Agencia Estatal Boletín Oficial del Estado, Madrid, 2018

E. Herlin-Karnell (2012), *The constitutional dimension of European Criminal Law*, Hart Publishing, 2012

V.C. Jackson (2015), *Constitucional Law in an Age of Proportionality*, in "The Yale Law Journal", vol. 124, 2015, n. 8

J. León Camacho (2020), *Evolución y desarrollo de los derechos humanos. Hacia una cuarta generación*, in R. Miranda Gonçalves, G. Martín Rodríguez, F. da Silva Veiga et al. (eds.) "El Derecho Público y Privado Ante las Nuevas Tecnologías", Editorial Dykinson, 2020

P. Martín Ríos (2017), *La indemnidad del domicilio informático como posible límite a la digital forensics*, in L. Mezzetti, E. Ferioli (a cura di), "Giustizia e Costituzione agli albori del XXI Secolo", Bonomo Editore, 2017

E. Martellozzo, E.A. Jane (2017), *Cybercrime and its Victims,* Routledge Studies in Crime and Society, 2017

H. Miranda Bonilla (2016), *El acceso a Internet como derecho fundamental*, in "Revista Jurídica IUS Doctrina", 2016, n. 15

P. Morales Aguilera (2018), *Entre el prisma discursivo y el ciberhumanismo: algunas reflexiones sobre Derechos Humanos de cuarta generación*, in "Franciscanum", vol. LX, 2018, n. 169

L. Nannipieri (2013), *Profili costituzionali dell'accesso ad Internet*, doctoral thesis supervised by R. Romboli, Università di Pisa, 2013

L. Picotti, R. Flor, I. Salvatori (2021), *Gruppo VII, Reati contro l'inviolabilità del domicilio, la tutela della vita privata e dei segreti, la libertà e la personalità informatica. Sottogruppo: Reati contro la riservatezza e la sicurezza informatiche, nonché l'identità digitale*, Università di Veronain "www.aipdp.it", 2021

R. Pisa (2010), *L'accesso ad Internet: un nuovo diritto fondamentale?,* in "Treccani Magazine", 12 gennaio 2010

O. Pollicino (2023), *The Right to Internet Access. A comparative Constitutional Legal Framework*, in "The Cambridge Handbook of Information Technology, Life Sciences and Human Rights", Cambridge University Press, 2023

O. Pollicino, G. Romeo (2016), *The Internet and Constitutional Law. The protection of fundamental rights and constitutional adjudication in Europe*, Routledge, 2016

L. Puente Rodríguez (2019), *Consecuencias del carácter procesal del "fraude de etiquetas": especial referencia a la libertad vigilada*, in "Revista General de Derecho Procesal", 2019, n. 47

J. Rifkin (2000), *The Age of Access: The New Culture of Hypercapitalism, Where All of Life is Paid-For Experience*, New York, 2000

J.C. Riofrío Martínez Villalba (2014), *La Cuarta Ola de Derechos Humanos: Los Derechos Digitales*, in "Revista Latinoamericana de Derechos Humanos", vol. 25, 2014, n. 1

S. Rodotà (2012), *Il diritto di avere diritti,* Laterza, 2012

K. Starr (2025), *Negligent delegation of digital enforcement by sovereign governments™: A framework for global constitutional accountability in privatized enforcement systems.* KStarr Enterprises, LLC, 2025

S. Signorato (2018), *Le indagini digitali. Profili struttural di una metamorfosi investigativa*, Giappichelli, 2018

M. Torre (2019), *Indagini informatiche e principio di proporzionalità*, in "Processo penale e giustizia", 2019, n. 6

M. Torre (2015), *Il virus di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in "Rivista Diritto penale e processo", vol. 21, 2015

M. Trogu (2019), *Intrusioni segrete nel domicilio informatico*, in A. Scalfati (a cura di), "Le indagini atipiche", Giappichelli, 2019

E. Velasco Núñez (2012), *Medidas restrictivas en Internet: cómo retirar contenidos ilícitos*, in M. Bauzá Reilly, F. Bueno de Mata (coord.), "El derecho en la sociedad telemática. Estudio en homenaje al profesor Valentín Carrascosa López", Andavira, 2012

A. Venegoni, I. Giordano, (2016), *La Corte costituzionale tedesca sulle misure di sorviglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, in "Diritto Penale Contemporaneo", 8 maggio 2016

RIVISTA ITALIANA
DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0251 • articolo sottoposto a peer review • pubblicato in anteprima il 19 dic. 2025

Antonio Iannuzzi

Lingua del diritto, lingua dell'Intelligenza Artificiale. Una prima riflessione

L'articolo esplora il rapporto tra la lingua del diritto e quella dell'Intelligenza Artificiale (AI) nel contesto della società digitale, un tema di crescente rilevanza nel campo del costituzionalismo democratico. Si evidenzia infatti come l'introduzione delle tecnologie digitali stia creando una crescente distanza fra questi due linguaggi, che, pur essendo inizialmente difficili da integrare, sono cruciali per garantire il corretto esercizio dei diritti fondamentali nell'ecosistema digitale. La riflessione si basa sull'idea che la trasformazione sociale provocata dall'AI abbia effetti significativi sulla lingua, sollevando interrogativi su come questa nuova tecnologia influenzerà il linguaggio giuridico e viceversa. L'articolo affronta, quindi, il tema della necessità di un dialogo tra la cultura letterario-umanistica e quella scientifico-tecnica, sottolineando che una comunicazione adeguata è essenziale per il corretto funzionamento del diritto nell'era digitale. Infine, l'autore propone l'uso delle Intelligenze Artificiali generative, come i Large Language Models (LLM), per facilitare la comunicazione tra questi due mondi, migliorando la comprensione del diritto e la trasparenza delle decisioni dell'AI nell'ambito giuridico, richiamando tuttavia l'attenzione sulla necessità di promuovere e tutelare la lingua italiana.

Lingua del diritto – Intelligenza Artificiale – Costituzionalismo democratico – Ecosistema digitale
Large Language Models (LLM)

The Language of Law, the Language of Artificial Intelligence. A first reflection

This article examines the relationship between the language of law and that of Artificial Intelligence (AI) within the context of the digital society, a subject of increasing relevance in the field of democratic constitutionalism. It underscores the fact that the introduction of digital technologies is gradually creating a growing divide between these two languages, which, although initially difficult to reconcile, are crucial for ensuring the proper exercise of fundamental rights within the digital ecosystem. The analysis is grounded in the premise that the social transformation brought about by AI has significant implications for language, raising pertinent questions regarding how this new technology will impact legal language and vice versa. The article, therefore, addresses the necessity of fostering dialogue between the humanistic-literary culture and the scientific-technical culture, emphasizing that effective communication is indispensable for the proper functioning of law in the digital era. Lastly, the author advocates for the use of generative Artificial Intelligence, particularly Large Language Models (LLMs), as a means to facilitate communication between these two realms, thereby enhancing both the understanding of legal concepts and the transparency of AI decision-making within the legal domain, while also highlighting the importance of promoting and safeguarding the Italian language.

Language of law – Artificial Intelligence (AI) – Democratic constitutionalism – Digital ecosystem
Large Language Models (LLMs)

L'Autore è professore ordinario di Istituzioni di diritto pubblico presso l'Università degli Studi Roma Tre
Questo contributo è destinato alla pubblicazione nel *Liber amicorum* per Michele Ainis

1. "Due culture", due lingue

Il rapporto fra lingua e diritto tocca diverse questioni del costituzionalismo democratico[1]. Il presente contributo mira ad esaminare un profilo specifico ed attuale della questione: i condizionamenti reciproci che si determinano fra la lingua del diritto e la lingua dell'Intelligenza Artificiale (AI) nella società digitale. La difficoltà di dialogo è inizialmente inevitabile, ma in un mondo sempre più dipendente dalle tecnologie digitali occorre evitare che si scavi un solco sempre più profondo fra i due mondi. La questione, perciò, merita di essere affrontata per facilitare una relazione semantica che è necessaria per diversi motivi. La ragione principale è che l'impostazione corretta di questa comunicazione influenza, come si vedrà, una delle precondizioni necessarie per l'effettivo esercizio di taluni diritti fondamentali nell'ecosistema digitale.

Di fronte ad una trasformazione così radicale della società, qual è quella innescata dall'avvento dell'AI, si rinnovano i riflessi negativi della frattura del sapere fra le "due culture"[2], che si è prodotta a partire dai primi del Novecento, e si rinverdiscono i timori paventati da tempo nella filosofia della scienza: "nessuno può essere, oggi, così cieco da non rendersi conto che l'esistenza di due culture, tanto diverse e lontane una dall'altra quanto la cultura letterario-umanistica e quella scientifico-tecnica, costituisce un grave motivo di crisi della nostra civiltà; essa vi segna una frattura che si inasprisce di giorno in giorno, e minaccia di trasformarsi in un vero muro di incomprensione, più profondo e nefasto di ogni altra suddivisione"[3].

Il presente saggio prende le mosse dalla constatazione che, poiché la tecnologia ha, non da oggi, un potere trasformativo della realtà, l'AI produrrà effetti sulla lingua. Da questa evidenza si solleva un ventaglio di domande: (i) una tecnologia dirompente qual è l'AI che effetti produrrà sulla lingua del diritto?; (ii) la lingua dell'AI saprà evolvere acquisendo la complessità gergale che connota la lingua del diritto?; (iii) quest'ultima come si adatterà alla lingua dell'AI?

Nella parte finale del lavoro rifletterò sul possibile utilizzo delle Intelligenze Artificiali generative e specialmente dei Large Language Models (LLM) per facilitare il dialogo fra i due mondi. L'utilizzo di questi sistemi potrebbe produrre due effetti positivi. In primo luogo, potrebbe aiutare a veicolare la conoscenza del diritto e facilitare la comprensione del diritto da parte dei destinatari. In secondo luogo, potrebbe agevolare la conoscibilità delle decisioni dell'AI che saranno utilizzate sempre di più nell'ambito giuridico nella società digitale.

2. La lingua del diritto: dal linguaggio comune a gergo tecnico

La differenza fra la lingua del diritto e quella dell'AI è notevole poiché esse germinano da linguaggi

1. A conferma della centralità del tema, nell'abbondante letteratura, si può fare riferimento ad Aa. Vv. 2023.
2. Snow 1964.
3. Geymonat 1964, pp. VII e XIV.

diversi e poi si distanziano ancor di più evolvendo in linguaggi settoriali e tecnici.

Diversamente che l'AI che basa il suo linguaggio sulla matematica, tradizionalmente il diritto, come ha acutamente messo in luce Michele Ainis, si serve del linguaggio comune, con la sua "carica d'indeterminazione", che è il portato del fatto che "esso serve a parlare della vita, e deve essere pertanto duttile, e in un certo senso vago, per riuscire a esprimere tutte le circostanze che di volta in volta ci coinvolgono"[4].

Per assolvere alla sua funzione, il linguaggio del diritto evolve poi in un gergo tecnico, settoriale, "e lo fa proprio allo scopo di temperare la naturale ambiguità del linguaggio comune rendendolo maggiormente vincolante, cercando quindi di guadagnare una maggiore precisione, che a sua volta tende a conquistare la certezza"[5].

Se il diritto deve aspirare alla chiarezza, alla certezza e alla prevedibilità per essere compreso e applicato dalla generalità dei consociati, man mano che progredisce e che affina i suoi strumenti produce un effetto che è stato efficacemente definito, ancora da Ainis, come un "paradosso": "s'allontana dalla possibilità di raggiungere tutti i consociati, e perde dunque la forza vincolante, in capacità prescrittiva, proprio mentre si sforza di raggiungerla. In qualche modo, la *forma* delle regole giuridiche tradisce dunque la loro specifica *funzione*; e questo fenomeno è destinato a estendersi man mano che le conoscenze giuridiche diventano via via più raffinate, più sofisticate". Questo percorso di evoluzione, che fatalmente appunto lo allontana dalla comprensione diffusa da parte della generalità dei consociati, si produce perché il diritto diventa una scienza, reificando proprio quel "paradosso" per cui "per prosperare lo sviluppo delle conoscenze richiede infatti un clima pluralista e democratico, ove le informazioni circolino liberamente e senza veti, e ne sia possibile il reciproco controllo; sennonché, man mano che si procede verso nuove acquisizioni, aumenta il tasso di complessità e la scienza diventa in ultimo sempre più oligarchica e lontana dagli ideali democratici, posto che soltanto pochi specialisti saranno poi in grado di comprenderne il linguaggio"[6].

3. Intersezioni fra la lingua del diritto e la lingua dell'Intelligenza Artificiale fra divergenze e convergenze

Il diritto interseca la lingua della tecnica con sempre maggiore frequenza.

Al cospetto delle fattispecie a contenuto tecnico-scientifico la biforcazione linguistica tende ad ampliarsi in ragione della tecnicità intrinseca dell'oggetto della regolazione. La fondamentale conoscenza della materia da regolare comporta la necessità per il giurista di acquisire termini propri di altre branche del sapere. La regolazione di ambiti tecnico-settoriali richiede, poi, un utilizzo di lemmi non propri del linguaggio giuridico, finendolo per condizionare.

Da questo punto di vista, la lingua del diritto è aperta ai condizionamenti esterni e muta adattandosi al contesto sociale.

In una fase di transizione verso una società digitale e dell'AI, il diritto sempre di più finisce per essere permeato da cognizioni informatiche espresse mediante linguaggi tecnici o matematici.

Nell'ecosistema digitale, in special modo, il legislatore avverte la necessità, se non talvolta l'obbligo, di confrontarsi con esperti di altri rami del sapere, come l'ingegnere informatico o l'esperto di dati. Si fa strada sempre di più la necessità di lavorare in contesti multidisciplinari. Anche sotto questo aspetto si produce un paradosso: in un momento in cui la conoscenza si parcellizza e la formazione universitaria o scientifica tende alla specializzazione, comprendere l'ecosistema digitale richiede uno sguardo ampio ed un approccio interdisciplinare. In un diverso contesto metodologico occorre favorire un dialogo con esperti di diversi settori che non è né spontaneo né semplice da realizzare perché ciascuno acquisisce un lessico specialistico e forbito, che tante volte ostacola la comprensione reciproca.

Nella società digitale, con l'avvento dell'Intelligenza Artificiale, la forbice fra la lingua del diritto e la lingua della tecnologia rischia fatalmente di allargarsi ancora di più.

Il problema di partenza deriva dal fatto che i linguaggi algoritmici sono linguaggi di

4. Ainis 2013, p. 61.
5. *Ibidem*.
6. *Ivi*, p. 61-62.

programmazione fondati sulla matematica. Questi ultimi, peraltro, spesso adottano un inglese tecnico internazionale.

Mentre il linguaggio giuridico è aperto e duttile, quello algoritmico è "sempre un sistema "chiuso", nel senso che non può dar luogo, come accade invece nei linguaggi "naturali", a nuove espressioni o a nuove strutture di frasi: la sua grammatica stabilisce a priori l'insieme, anche infinito, delle sue espressioni sintatticamente corrette. Questo perché un linguaggio algoritmico "deve essere sempre interpretabile dal linguaggio algoritmico più basso, dai software interpreti, dai software compilatori e, infine, dalla macchina"[7]. La lingua del diritto e la lingua dell'Intelligenza Artificiale sono entrambe altamente specializzate, ma si distanziano per obiettivi, struttura e uso del linguaggio.

Il diritto che, come detto, tradizionalmente evolve dal linguaggio comune, in questo caso ha invece necessità di confrontarsi con un linguaggio "non naturale". Il rischio è che si determini da una parte un problema di "inconciliabilità" fra la lingua del regolante e quella del regolato, dall'altra parte una grave e dilagante incomprensibilità della norma giuridica da parte dei destinatari. Si potrebbero fare decine di esempi, ma penso che basti fare riferimento alla difficoltà quotidiana di districarsi nella decisione se concedere il consenso ai cookies di navigazione su Internet a fronte del fatto che la gran parte degli utenti non ha piena contezza di cosa sia tecnicamente un cookie e di cosa comporti in concreto fornire il consenso all'installazione di un cookie di profilazione. Detta difficoltà di comprensione è un problema che riguarda sia il legislatore sia i cittadini. Manca in questi ultimi una diffusa educazione al digitale che accompagni di pari passo la transizione digitale, che invece è necessaria per dare consapevolezza ai cittadini delle opportunità offerte dalle tecnologie emergenti e dei rischi connessi, in modo da consentire di effettuare scientemente le scelte individuali e di godere pienamente dei diritti fondamentali nell'ecosistema digitale.

La forbice fra il linguaggio del diritto e quello dei sistemi di AI può determinare diversi problemi, fra cui, esemplificativamente e riassuntivamente, si segnalano: (1) le difficoltà che incontra il legislatore nel regolare gli oggetti della società digitale; (2) i problemi nell'applicazione del diritto, che emergono nell'esercizio della giurisdizione; (3) le complicazioni nella comprensione della norma giuridica da parte dei destinatari; (4) l'aggravamento della fatica per lo svolgimento della già difficile attività di divulgazione legislativa; (5) la più ardua maturazione del diritto individuale all'autodeterminazione informativa.

È bene notare, però, che i due linguaggi hanno anche qualche importante punto di contatto. L'algoritmo matematico si basa su una formula logica che produce una sequenza di operazioni per arrivare ad un risultato che, se ci si pensa bene, non è una formula distante da quella che è alla base della struttura della norma giuridica. Nell'ordinamento giuridico molte norme al fine dispongono di produrre determinati effetti legali, in dipendenza del verificarsi di certe situazioni. Lo schema è, comunque, sempre quello che si esprime nella formula kelseniana *se (a), allora (b)*: dove (a) è una situazione verificata come reale (es., se commetti un omicidio allora sei punito con la reclusione fino a 24 anni). Ancora meno distanza si registra tra il linguaggio dell'AI e quello della norma tecnica, che con frequenza si applica nell'ecosistema digitale, se si pensa alla proposta di Vezio Crisafulli, secondo il quale la norma tecnica è figura tipologicamente distinta dalle leggi di natura e da quelle della pratica, perché capovolge lo schema causale della corrispondente legge naturale (*se c'è A, c'è B*) in termini prescrittivi (*se si vuole B, si deve porre in essere A*)[8].

Se si assume l'idea che esistono anche decisivi punti di contatto, allora il rapporto tra la lingua del diritto e quella dell'algoritmo di AI non appare irriducibile.

Anche nell'utilizzo dell'AI ci sono avvicinamenti più considerevoli di altri. È stato attentamente osservato, in proposito, che "allineando la logica algoritmica al ragionamento giuridico, gli algoritmi condizionali possono essere utilizzati per supportare o automatizzare i processi decisionali amministrativi in modo compatibile con i quadri giuridici esistenti. Se progettati e implementati correttamente, questi algoritmi possono migliorare l'efficienza, la coerenza e la trasparenza

7. Cavaggion–Orofino 2023, p. 173 ss.

8. Crisafulli 1970, p. 12.

delle azioni amministrative, pur rispettando i principi giuridici sottostanti"[9].

4. Ecosistema normativo digitale e spinte in favore di un dialogo fra le "due lingue"

Nell'ecosistema normativo digitale ci sono diversi principi che obbligano ad assumere una prospettiva metodologica interdisciplinare ed impongono un dialogo fra giuristi ed informatici (e non solo…). Mi limito a menzionare i principali.

Il primo è l'approccio *by design* che, innanzitutto, ha introdotto il Regolamento (UE) 2016/679 (GDPR). L'art. 25 stabilisce che il Titolare del trattamento deve valutare, sin dalla progettazione del trattamento, i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento; allo stesso tempo deve mettere in atto misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati e ad integrare nel trattamento le necessarie garanzie al fine di tutelare i diritti degli interessati[10]. Tale approccio si estende ai produttori di prodotti, servizi e applicazioni che "dovrebbero essere incoraggiati", fin dalla progettazione, "a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati" (considerando 78). L'approccio *by desig*n, che si estende ad altri ambiti della regolazione digitale (rischio, etica, sicurezza, ecc.), impone allora la presenza di un giurista all'interno dei sistemi di produzione, impostando così una collaborazione stabile e necessaria fra profili tecnici e giuridici. Tale cooperazione non si esaurisce nella fase prodromica della progettazione del trattamento o del prodotto, ma deve estendersi a tutta la durata del trattamento. I rapporti fra giuristi e tecnici diventano capillari così che i "linguaggi si mescolano"[11]. È fondamentale, invece, acquisire la capacità di lavorare in ambienti multidisciplinari perché "per risolvere le grandi sfide che la società deve affrontare – energia, acqua, clima, cibo, salute – scienziati e scienziati sociali devono lavorare insieme"[12]. Relativamente all'approccio *by design* è stato sostenuto, utilizzando l'esempio della limitazione di velocità preimpostata nelle auto a guida autonoma, come questa tecnica normativa possa anche comportare la riduzione dell'attività dell'uomo perché "l'obiettivo normativo (…) viene 'confezionato' all'interno degli strumenti tramite i quali l'infrazione di tale obiettivo, sebbene soltanto tramite l'intervento umano, risultava precedentemente possibile"[13].

Un secondo esempio di abbraccio obbligato e forte fra i due linguaggi si ha allorché vengono in applicazione i principi di trasparenza (conoscibilità), spiegabilità e di intervento umano (art. 22 GDPR; art. 5 Regolamento (UE) 2024/1689, c.d. AI ACT). Per comprendere meglio l'origine e il senso del problema è utile fare riferimento, fra i tanti, ad un caso giurisprudenziale, perché fa emergere, in modo estremamente esemplare, la difficoltà di conciliare i due diversi linguaggi. Il caso ha origine in occasione dell'applicazione della legge n. 107/2015 (c.d. "Buona scuola"), allorché la giurisprudenza amministrativa è stata chiamata alla travagliata elaborazione di un diritto di accesso al codice sorgente dei sistemi di AI. Uno degli aspetti più controversi derivanti dall'applicazione della legge è stato il funzionamento dell'algoritmo sulla base del quale è stata decisa l'assegnazione delle cattedre, che ha gestito la mobilità dei docenti su scala nazionale. Molti insegnanti hanno lamentato errori e disparità, con assegnazioni lontane dalle proprie province, in base a criteri oscuri ed apparentemente arbitrari. La prima questione che si è posta ha investito proprio la trasparenza della procedura algoritmica, poiché molti insegnanti hanno presentato istanza formale di accesso al codice sorgente dell'algoritmo decisionale, in quanto atto amministrativo informatico, ai sensi dell'art. 22 della legge n. 241/1990, contro il diniego

9. Così Carullo 2023.
10. In tema Calzolaio 2017.
11. Tallacchini 2012, p. 315.
12. Santosuosso 2020, p. 153 s. Condivisibilmente, segnala l'A. che "la capacità di lavorare in team interdisciplinare vale più di mere nozioni" (p. 151 ss.).
13. Lucy 2023, p. 18.

opposto dal Ministero dell'Istruzione, al fine di poter conoscere il funzionamento del sistema e di avere evidenza di eventuali errori di valutazione o di discriminazioni involontarie.

Le argomentazioni poste alla base del diniego espresso dall'amministrazione all'istanza di accesso facevano leva sulla non assimilabilità del codice sorgente del software "in quanto sostanziantesi in un testo di un algoritmo di un programma scritto in un linguaggio di programmazione, compreso all'interno di un file" e non in un "documento amministrativo", inteso ai sensi dell'art. 22, lett. d), della legge n. 241/1990.

A fronte dei ricorsi presentati, il TAR Lazio[14] ha riconosciuto, invece, il diritto di accesso algoritmico, ma i ricorrenti a quel punto si sono ritrovati in mano non un documento amministrativo scritto con i canoni linguistici del diritto, ma un codice sorgente algoritmico di non comune comprensione. Per "decifrare" il "geroglifico informatico" è stato necessario acquisire i pareri di esperti tecnici. Va detto, per inciso, che gli oneri a carico delle parti finiscono, in casi analoghi, per aggravare l'esercizio del diritto costituzionale di difesa. Al riguardo, infatti, non appare ancora sufficiente il riconoscimento del diritto di accesso al codice sorgente dell'algoritmo perché occorre invece assicurare un più penetrante diritto di accesso assistito, come non ha tardato a fare il Consiglio di Stato, che ha affermato che "il meccanismo con cui si concretizza la decisione robotizzata" dev'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", nonché che la logica dell'algoritmo deve essere "non solo conoscibile in sé, ma anche soggetta alla piena cognizione, e al pieno sindacato, del giudice amministrativo"[15]. In questa prospettiva è condivisibile la proposta di "una lettura non riduttiva dell'art. 24 Cost." che "imponga sul piano costituzionale l'obbligo per le tecnologie 'sociali' di utilizzare linguaggi umanamente comprensibili, come precondizione necessaria per la garanzia (giurisdizionale e non) dei diritti nelle aree di libertà 'incise' da tali tecnologie"[16].

5. Utilizzo dei LLM per agevolare il principio della conoscibilità dei sistemi di AI

Quest'ultima affermazione giurisprudenziale mostra che è l'Intelligenza Artificiale che deve avvicinarsi alla lingua del diritto per assicurare pienamente il principio di conoscibilità, in una prospettiva di evoluzione della lingua dell'AI che deve auto-apprendere i tecnicismi del linguaggio giuridico. Questo compito oneroso oggi può essere meglio assolto dai Large Language Model (LLM) che si stanno sviluppando e diffondendo con grande velocità. Com'è noto si tratta di sistemi di *machine learning* in grado di elaborare risposte utilizzando un registro linguistico capace di generare un linguaggio comune. La strada della lingua del diritto e quella dell'AI sembrano intersecarsi grazie a questi sistemi, agevolando un dialogo più continuo e non necessariamente mediato da esperti.

È bene essere consapevoli, però, che i modelli LLM hanno una capacità linguistica che ancora mantiene importanti differenze con il linguaggio del diritto, per due ragioni più evidenti di altre.

La prima ragione è che i sistemi LLM propongono un linguaggio che sembra "naturale", ma che alla base è il prodotto di un modello statistico che si basa, in grosso modo, sulla percentuale che la parola successiva sia scelta fra quelle che più probabilmente possono seguire la precedente.

La seconda ragione solleva un problema peculiare dell'ordinamento giuridico italiano, vale a dire che tali sistemi sono impostati per parlare meglio in lingua inglese, allo stato attuale dello sviluppo. Questo per via del fatto che l'addestramento delle LLM è più ricco e approfondito in inglese, perché la maggior parte dei dati reperibili pubblicamente su Internet è disponibile in quella lingua. Perciò

14. TAR Lazio, sez. III bis, sent. 22 marzo 2017, n. 3769. Cfr. Cons. Stato, sez. VI, sent. 4 febbraio 2020, n. 881 che ha ulteriormente rafforzato l'importanza della trasparenza nell'uso di sistemi automatizzati, sottolineando che l'accesso alle informazioni relative agli algoritmi è fondamentale per garantire la legittimità e la comprensibilità dell'azione amministrativa. Ma vedi ora, sulla questione, la nuova posizione del Cons. Stato, sezione IV, sentenza del 4 giugno 2025, n. 4857.
15. Cons. Stato, sez. VI, sent. 8 aprile 2019, n. 2770.
16. Simoncini 2023, p. 168 ss.

detti sistemi possono offrire risposte in inglese più dettagliate, con più sfumature linguistiche e maggiore accuratezza. Le risposte tecniche in italiano, come in molte altre lingue, presentano, al momento, un livello di qualità solo accettabile.

Apprendo dall'esame del funzionamento tecnico dei sistemi AI *detector*, che sono quelli che aiutano ad indagare se un testo è stato generato da LLM, che il risultato che pongono in essere (anch'esso di tipo probabilistico) è possibile per via della presupposizione della povertà del registro linguistico dei primi rispetto alla ricchezza del lessico e delle capacità espressive dell'uomo. Questo deficit linguistico dell'AI si può ascrivere alla giovane età dei LLM, ed in questa prospettiva si può immaginare che sarà progressivamente limitato; ma si può anche imputare al meccanismo che genera un linguaggio comune partendo da un'elaborazione matematica. In questa seconda ipotesi prevedibilmente potrebbe permanere una qualche forma di biforcazione linguistica.

6. Tutelare e promuovere la lingua italiana, curare la lingua del diritto

Il processo di contaminazione progressivo tra la lingua del diritto e la (neo)lingua dell'AI produrrà conseguenze che saranno pienamente valutabili solo in futuro. Non è difficile, tuttavia, già da ora scorgere alcuni segnali del cambiamento in atto, ponendo attenzione al fatto che il rapporto di condizionamento sarà inevitabilmente reciproco obbligando, quindi, anche il diritto ad adattarsi e mutare.

Allo stato attuale del funzionamento, la "povertà" linguistica dell'AI può ingenerare diversi problemi al diritto.

In primo luogo, un suo uso diffuso da parte della popolazione e della più stretta cerchia dei chierici del diritto può provocare potenzialmente un impoverimento linguistico diffuso nella popolazione o negli specialisti, perché costretti ad un dialogo svilente e necessariamente adattivo.

Lo aveva preconizzato Italo Calvino parlando dell'avvento della "antilingua", ossia di quell'italiano surreale che aveva contagiato il nostro linguaggio quotidiano, per effetto della mancanza degli uomini di un vero contatto con la vita, ciò che è problema acuito nella società digitale e dell'Intelligenza Artificiale. Scriveva Calvino che "Ogni giorno, soprattutto da cent'anni a questa parte, per un processo ormai automatico, centinaia di migliaia di nostri concittadini traducono mentalmente con la velocità di macchine elettroniche la lingua italiana in un'antilingua inesistente.

Avvocati e funzionari, gabinetti ministeriali e consigli d'amministrazione, redazioni di giornali e di telegiornali scrivono parlano pensano nell'antilingua. (…) Perciò dove trionfa l'antilingua – l'italiano di chi non sa dire "ho fatto" ma deve dire "ho effettuato" – la lingua viene uccisa"[17].

In secondo luogo, la diffusione dei sistemi di AI può contribuire, per le ragioni dette, ad un'ulteriore spinta verso l'uso dell'inglese in luogo della lingua italiana conducendo ad uno svilimento ulteriore della lingua italiana intesa come fattore identitario.

Questi rischi sono stati lucidamente messi in risalto, con la massima autorevolezza possibile, dal Presidente della Repubblica che, in un'occasione pubblica ha sostenuto: "La lingua è chiave di accesso a uno specifico culturale straordinario dispiegatosi nei secoli e offerto alla comunità umana nelle sue espressioni più alte: la scienza, l'arte in ogni sua forma, gli stili di vita. La lingua è anche strumento di libertà e di emancipazione: l'esclusione nasce dalla povertà delle capacità di esprimersi, dei patrimoni lessicali. La sudditanza si alimenta della cancellazione delle parole e con la sostituzione di esse con quelle del dispotismo di turno. Va evitato il rischio, che si potrebbe fare ancora più alto con l'avvento dell'Intelligenza Artificiale, di diminuire il pluralismo linguistico, con il conseguente depauperamento del patrimonio culturale che gli idiomi veicolano, a favore di neo linguaggi con vocazione esclusivamente funzionale alla mera operatività digitale"[18].

Sono parole che si pongono in linea con la giurisprudenza della Corte costituzionale che ha statuito in più di un'occasione che la lingua è "elemento fondamentale di identità culturale e […] mezzo primario di trasmissione dei relativi

17. Calvino 1995, p. 149 ss.

18. Si veda il comunicato relativo al "Messaggio del Presidente Mattarella in occasione del quarantesimo anniversario di nascita della Comunità Radiotelevisiva Italofona" nel sito della Presidenza della Repubblica.

valori"[19]; "elemento di identità individuale e collettiva di importanza basilare"[20] e non può essere posta "in posizione marginale"[21] rispetto alle altre, nemmeno per effetto della "progressiva integrazione sovranazionale degli ordinamenti" e dell'"erosione dei confini nazionali determinati dalla globalizzazione" che "possono insidiare senz'altro, sotto molteplici profili, tale funzione della lingua italiana"[22]. La lingua italiana, in definitiva, è "vettore della cultura e della tradizione immanenti nella comunità nazionale, tutelate anche dall'art. 9 Cost."[23], anche smascherando il falso "mito dell'internazionalizzazione" dietro cui si celano, in alcuni ambiti, politiche di inglesizzazione della cultura e della ricerca[24].

Sullo sfondo di staglia il monito orwelliano dell'introduzione della neolingua espresso nel celeberrimo romanzo *1984*. L'autore immagina profeticamente che una lingua artificiale venga imposta da un regime autoritario, che fonda il suo potere su una sorveglianza di massa e sulla manipolazione della verità, con l'obiettivo "di restringere al massimo la sfera d'azione del pensiero" ed impedire la ribellione, attraverso un'operazione di impoverimento del dizionario: "a ogni nuovo anno, una diminuzione nel numero delle parole e una contrazione ulteriore della coscienza"[25].

Promuovere e tutelare la lingua italiana, per le ragioni che si sono viste, significa prendersi cura anche della lingua del diritto.

Servirebbe, però, un'inversione di tendenza perché, com'è stato acutamente osservato, se andiamo alla ricerca degli interventi legislativi a "tutela dell'italiano, insieme alla promozione della sua conoscenza", scopriamo che "il paniere è quasi vuoto"[26]. È probabilmente il segnale di un'identità nazionale debole, incerta sui suoi stessi connotati, per l'appunto fin dagli esordi dello Stato unitario"[27]. Ma questa disattenzione contrasta con il modello costituzionale, perché la lingua, invece, va valorizzata, senza cadere nelle derive ideologiche, in quanto "è al tempo stesso un bene culturale, è insieme la memoria dei padri e l'orizzonte dei figli, ed è disgraziata la Repubblica che non abbia cura del proprio patrimonio culturale"[28].

Riferimenti bibliografici

Aa. Vv. (2023), *Lingua, linguaggi, diritti. Annuario 2022, Atti del XXXVII Convegno annuale. Messina-Taormina, 27-29 ottobre 2022*, Editoriale Scientifica, 2023

M. Ainis (2013), *La lingua del legislatore*, in S. Traversa (a cura di), "Scienza e tecnica della legislazione. Lezioni", Napoli, 2006, ora in M. Ainis, *Sette profili di diritto pubblico*, Jovene, 2013

M. Ainis (2010), *Politica e legislazione linguistica nell'Italia repubblicana*, in "Diritto pubblico", 2010

M.A. Cabiddu (2013), *La lingua e il mito (dell'internazionalizzazione)*, in "Diritto pubblico", 2013

I. Calvino (1995), *Saggi 1945-1985*, Mondadori, 1995

S. Calzolaio (2017), *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in "federalismi.it", 2017, n. 24

19. Corte cost., sent. 5 febbraio 1992, n. 62.
20. Corte cost., sent. 22 gennaio 1996, n. 15.
21. Corte cost., sent. 18 maggio 2009, n. 159.
22. Corte cost., sent. 18 maggio 2009 n. 159.
23. Corte cost., sent. 21 febbraio 2017, n. 42.
24. Cabiddu 2013.
25. Orwell 2016.
26. Ainis 2010, p. 176.
27. *Ibidem*.
28. *Ivi*, p. 193.

G. Carullo (2023), *Large Language Models for Transparent and Intelligible AI-Assisted Public Decision-Making*, in "Ceridap", 2023, n. 3

G. Cavaggion, M. Orofino (2023), *Lingua e Costituzione. L'irrompere dei linguaggi algoritmici,* in "Rivista AIC", 2023, n. 4

V. Crisafulli (1970), *Lezioni di diritto costituzionale, I, Introduzione al diritto costituzionale italiano*, Cedam, 1970

L. Geymonat (1964), *Prefazione*, in C.P. Snow, "Le due culture", trad. it., Feltrinelli, 1964

W. Lucy (2023), *La morte del diritto. Ancora un necrologio*, Edizioni Scientifiche Italiane, 2023

G. Orwell (2016), *1984*, Mondadori, 2016

A. Santosuosso (2020), *Intelligenza Artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Mondadori, 2020

A. Simoncini (2023), *Il linguaggio dell'intelligenza artificiale e la tutela costituzionale dei diritti,* in Aa. Vv., "Lingua, linguaggi, diritti. Annuario 2022, Atti del XXXVII Convegno annuale. Messina-Taormina, 27-29 ottobre 2022", Editoriale Scientifica, 2023

C.P. Snow (1964), *Le due culture*, trad. it., Feltrinelli, 1964

M. Tallacchini (2012), *Scienza e diritto. Prospettive di co-produzione*, in "Rivista di filosofia del diritto", 2012

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0256 • articolo sottoposto a peer review • pubblicato in anteprima il 23 dic. 2025

Kreshnik Vukatana – Elira Hoxha – Anxhela Ferhataj

Ethical integration of AI in judicial systems: Advancing fairness, transparency, and judicial efficiency

This study assesses the perceived role of Artificial Intelligence (AI) in advancing judicial reform in Albania, with emphasis on efficiency, fairness, and transparency. A survey of 340 students in law, computer science, and computer engineering was analysed using Spearman's rank correlation to explore how perceived benefits and risks relate to support for AI in justice processes. The findings show a balanced view. Students acknowledge AI's potential to reduce delays and improve administrative coordination, yet they also express concerns about bias, limited transparency, and relying on automated tools in decisions that affect fundamental rights. They emphasise the need for clear rules, explainable systems, and strong human oversight to ensure responsible use. This research makes a pioneering contribution to understanding how future legal professionals perceive AI in transitional judicial systems, introducing an AI-Driven Justice System Framework based on the study's findings.

AI in Justice Systems – AI Ethics – Fairness – Transparency in AI – Judicial Efficiency

Integrazione etica dell'intelligenza artificiale nei sistemi giudiziari: promuovere equità, trasparenza ed efficienza giudiziaria

Questo studio analizza il potenziale dell'IA nel trasformare i sistemi giudiziari, con riferimento al contesto albanese. Un sondaggio su 340 studenti di giurisprudenza e area tecnico-informativa, esaminato tramite correlazione di Spearman, indaga il legame tra benefici e rischi percepiti e il supporto all'IA nei processi giudiziari. I risultati mostrano un cauto ottimismo rispetto alla capacità dell'IA di migliorare efficienza e ridurre i ritardi, insieme a rilevanti preoccupazioni sulla correttezza degli algoritmi impiegati, trasparenza decisionale e necessità di supervisione umana. Questa ricerca contribuisce a chiarire come i futuri professionisti valutino l'integrazione dell'IA nei sistemi giudiziari, introducendo un *AI-Driven Justice System Framework* elaborato sulla base dei risultati dello studio.

IA nei sistemi giudiziari – Etica dell'IA – Equità – Trasparenza dell'IA – Efficienza giudiziaria

Kreshnik Vukatana is an Associate Professor of Computer Science and the Head of the Department of Statistics and Applied Informatics at the Faculty of Economy, University of Tirana. Elira Hoxha is an Associate Professor at the Department of Statistics and Applied Informatics, Faculty of Economy, University of Tirana. Anxhela Ferhataj is Research Fellow at the Department of Statistics and Applied Informatics, Faculty of Economy, University of Tirana

1. Introduction

Artificial Intelligence (AI) is driving a global transformation in judicial systems, offering innovative solutions to support a more efficient use of judicial resources and to enhance fairness and access to justice[1]. By automating routine processes and analyzing large datasets, AI technologies, including predictive algorithms[2], sentencing recommendation systems, and parole risk assessment tools, show clear promise for improving legal operations and addressing systemic inefficiencies. However, these advancements raise tough ethical, legal, and social questions[3]. Central to these challenges are concerns about fairness, accountability, and public trust[4]. In judicial systems already under scrutiny, AI raises pressing questions about its ability to uphold justice and protect fundamental rights.

Globally, AI's deployment in judicial systems has faced criticism for perpetuating biases embedded in historical data, disproportionately affecting marginalized communities and reinforcing societal inequities. The "black box" nature of many AI models, which are often opaque and difficult to interpret, compounds these concerns and undermines public trust[5]. This lack of transparency poses a direct threat to the principles of fairness and accountability essential to judicial integrity. These concerns are particularly critical in high-stakes areas such as criminal sentencing, parole decisions, and predictive policing, where the consequences of biased or opaque decisions can have severe

1. Lee 2025; Held–Habernal 2024; Dakalbab–Talib–Waraga et al. 2022.
2. Metsker–Trofimov–Kopanitsa 2021.
3. Barysė–Sarel 2024; Laptev–Feyzrakhmanova 2024; Simmons 2018.
4. Engel–Linhardt–Schubert 2025; Schweitzer–Conrads 2025; Di Porto–Fantozzi–Naldi–Rangone 2024.
5. Laptev–Feyzrakhmanova 2024.

and far-reaching impact[6]. As Marshall's study of the Horizon Post Office scandal demonstrates, a poorly understood and inadequately scrutinised IT system, treated as inherently reliable in court, contributed to widespread miscarriages of justice and highlights the legal and ethical risks that arise when digital systems in judicial proceedings are insulated from effective scrutiny[7].

In Albania, a nation undergoing substantial judicial reforms aimed at increasing efficiency and restoring public confidence[8], AI presents a unique opportunity to modernize legal processes. However, the success of these initiatives hinges not only on the technical implementation of AI but also on its societal acceptance and alignment with constitutional principles. Given their future roles as leaders in law, technology, and policymaking, university students provide valuable insights into society's readiness for adoption of AI in the judicial system. Albanian university students, drawn from law, information technology, and engineering disciplines, represent a critical demographic for understanding the broader implications of AI in the justice system. Their perspectives on algorithmic bias, transparency, and trust provide essential insights into the challenges and opportunities of AI-driven judicial innovations.

Despite the global discourse on AI's transformative potential in the legal field, there is a notable lack of empirical research examining the views of emerging stakeholders in transitional judicial systems such as the case of Albania. The CEPEJ mapping (Fig. 1) documents a growing number of AI tools across Europe, concentrated in low-risk workflow domains such as document search, triage, and transcription, yet Albania records no officially deployed AI systems in its courts. Precisely because the judiciary is still at a pre-adoption stage, this study is analytically important: it provides the first systematic account of how future legal and technology professionals in Albania evaluate the benefits, risks, and acceptable safeguards of judicial AI. By establishing an evidence-based baseline before tools are procured, the findings can inform the choice of use cases, the design of transparency and oversight requirements, and the sequencing of pilots, thereby guiding Albania's entry into judicial AI in a way that is aligned with both European standards and national expectations.

This study seeks to address this gap by exploring how Albanian university students perceive the integration of AI into Albanian judicial processes. Specifically, it investigates:

1. How do students perceive AI's potential to impact efficiency, fairness, and transparency in the justice system?
2. What concerns do students have regarding algorithmic bias, ethical implications, and societal impacts of AI in judicial decision-making?
3. How do students evaluate the role of transparency and accountability in fostering trust in AI-driven judicial systems?

By providing empirical insights into these critical questions, this research aims to advance global understanding of AI's role in justice. The findings will inform policymakers, legal practitioners, and technologists on designing AI systems that promote equity, fairness, and accountability, ensuring that AI integration into judicial systems aligns with fundamental legal principles.

2. Literature Review

The integration of AI into judicial systems is widely seen as transformative, with potential to streamline workflows, improve the timeliness of proceedings, and support a more efficient use of judicial resources, while increasing transparency[9]. AI has demonstrated its potential to streamline workflows, expedite case resolution, and reduce administrative burdens, making it a crucial tool for modernizing justice systems globally[10]. However, despite these benefits, AI deployment faces serious challenges, particularly regarding ethical governance, public trust, and equitable access. Ensuring that AI-driven reforms do not worsen existing

6. Bex 2025; Dakalbab–Talib–Waraga et al. 2022; Perrot 2017.
7. Marshall 2022.
8. European Commission for the Efficiency of Justice 2024.
9. Dakalbab–Talib–Waraga et al. 2022.
10. Metsker–Trofimov–Kopanitsa 2021; Nowotko 2021.

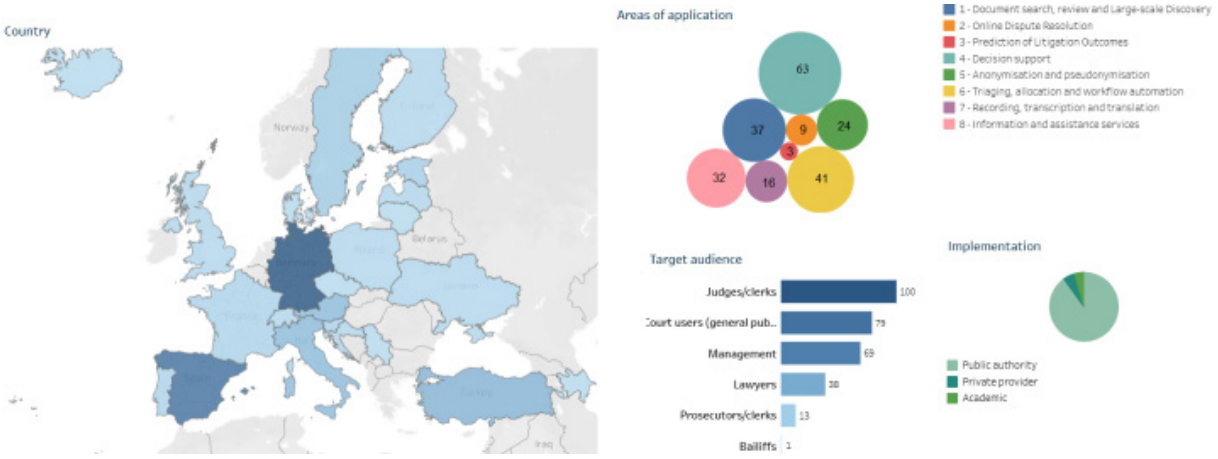

Fig. 1 — *Resource Centre Cyberjustice and AI By European Commission for the Efficiency of Justice (Council of Europe, European Commission for the Efficiency of Justice, Resource Centre on Cyberjustice and Artificial Intelligence, 2025)*

structural inequities or violate fundamental rights is vital.

In the case of Albania, a nation undergoing substantial judicial reforms to increase transparency and restore public trust, AI offers a promising opportunity. As Albania modernizes its legal infrastructure and addresses systemic inefficiencies[11], AI provides a practical pathway to achieving these goals while remaining consistent with constitutional principles and societal values.

2.1. AI's Role in Optimizing Judicial Efficiency and Workflows

Albania's efforts to address inefficiencies in its judicial system match global trends of leveraging AI to streamline workflows and reduce systemic backlogs. This alignment highlights Albania's potential to adapt international best practices for AI integration. Nowotko identifies the transformative role of advisory AI systems in civil and administrative cases, automating routine tasks such as electronic writs of payment[12]. This enables judges to focus on complex, discretionary cases, addressing a crucial need in Albania's reform-driven judiciary. Also, Nowotko warns against over-reliance on automated systems in criminal law, where maintaining fair trial principles and public trust is essential[13].

Metsker et al. stress the importance of text and data mining technologies in optimizing regulatory workflows. These tools can accelerate case analysis and improve access to legal precedents, reducing inefficiencies. However, challenges such as data inconsistencies, structural limitations, and stakeholder skepticism present serious barriers to broader adoption[14]. Their research calls for transparent, scalable, and interpretable machine learning (ML) systems that build trust and secure ethical AI integration into judicial processes. In Albania, where judicial backlogs remain an issue, such technologies could greatly support legal professionals and expedite case resolution[15].

In legal research, tools like *LaCour!*, introduced by Held and Habernal, demonstrate AI's potential to align oral arguments with judicial decisions. This tool enhances transparency by facilitating research in natural language processing (NLP) and enabling empirical analysis of dissent in judicial decision-making[16]. These innovations could im-

11. European Commission 2024.
12. Nowotko 2021.
13. *Ibidem.*
14. Metsker–Trofimov–Kopanitsa 2021.
15. European Commission for the Efficiency of Justice 2024.
16. Held–Habernal 2024.

prove transparency in Albania's judiciary, where opaque decision-making has eroded public trust. Similarly, Lee showcases *InstructPatentGPT*, which efficiently drafts legal documents, highlighting how AI tools tailored to legal domains can streamline workflows without sacrificing accuracy[17]. For Albania, adopting such tools could bridge gaps in expertise and resources, particularly in specialized legal areas.

Laptev and Feyzrakhmanova discuss the global capacity of AI to enhance organizational efficiency and decision-making[18]. Also, they caution that over-reliance on AI without defensible safeguards for transparency and accountability can be risky. They identify challenges such as algorithmic bias and data security vulnerabilities and advocate for a balanced approach that combines human oversight with AI to align with constitutional principles and make sure procedural fairness, thereby preserving public trust in judicial systems[19].

2.2. Ethical Challenges and Societal Implications

Integrating AI into Albania's judicial system requires addressing ethical concerns to make sure alignment with societal values and constitutional principles. Simmons highlights the potential of predictive algorithms in sentencing to perpetuate systemic biases. He emphasizes the need for algorithmic transparency and human oversight to ensure fairness[20]. In Albania, where judicial reforms are ongoing to address corruption and inequities, AI-driven decisions must sit with procedural justice. This shows the critical need for scrutinizing AI training datasets to prevent reinforcing pre-existing biases. Gless expands on these concerns, arguing that fully automated systems lack the interpretive nuance necessary for consequential judicial decisions, such as sentencing. He criticizes the use of robot judges, noting their inability to articulate "legal beliefs" that make sure compliance with fair trial standards[21]. Recent work on judicial decision-making and AI suggests that predictive and generative systems are not credible substitutes for the emotionally and cognitively grounded deliberation that underpins judicial reasoning, and should instead be treated as tools embedded in human-centred structures of oversight and accountability[22]. This makes clear the irreplaceable role of human judgment, particularly as Albania's judicial reforms focus on enhancing fairness and accountability.

Perrot explores the ethical challenges of predictive policing, warning against privacy infringements and the disproportionate targeting of marginalized communities. While AI-driven technologies enhance resource allocation and crime prevention, they pose risks, such as algorithmic bias and privacy violations. Perrot advocates for strong regulatory frameworks and human oversight to mitigate these risks, ensuring AI systems match ethical principles and societal values[23]. In Albania, balancing proactive law enforcement with effective oversight is critical to maintaining public trust in AI-driven solutions.

Bex presents a framework for integrating AI into legal systems, stressing the importance of collaboration across law, technology, and governance[24]. Drawing on insights from the Netherlands National Police Lab AI, Bex demonstrates how combining data-driven and knowledge-driven approaches can address ethical challenges while enhancing access to justice. His framework offers a roadmap for aligning AI development with societal values, ensuring fairness, accountability, and transparency in legal processes[25]. Recent research by Ferhataj et al. emphasizes the ethical awareness of Albanian university students regarding AI. Students express concerns about algorithmic transparency, data privacy, and the potential for AI to reinforce societal

17. Lee 2025.
18. Laptev–Feyzrakhmanova 2024.
19. *Ibidem.*
20. Simmons 2018.
21. Gless 2023.
22. Contini–Minissale–Bergman Blix 2024.
23. Perrot 2017.
24. Bex 2025.
25. *Ibidem.*

biases. They advocate for regulatory frameworks that prioritize accountability, transparency, and human oversight, critical for ensuring AI's alignment with legal and ethical principles[26].

Ilin and Kelli examine challenges surrounding AI-generated outputs and copyright in the EU, identifying issues such as lawful data access and ambiguous ownership. These challenges hinder innovation and necessitate regulatory reforms that balance innovation with ethical accountability[27]. Similarly, Szkalej and Senftleben advocate for tailored licensing frameworks to protect intellectual property while fostering innovation, offering valuable guidance for Albania as it integrates AI into its legal framework[28].

2.3. Transparency, Accountability, and Public Trust

Restoring public trust is crucial to Albania's judicial reforms, with transparency and accountability as central priorities in integrating AI within the judicial system. Engel, Linhardt, and Schubert highlight the challenges posed by opaque decision-making in tools like the *COMPAS* algorithm, which disproportionately affects underrepresented populations. They stress the importance of Explainable AI (XAI) models to improve interpretability and uphold constitutional accountability standards[29]. Their research advocates judicial oversight and public scrutiny to ensure fairness in AI decision-making. Drawing on an actor-network perspective, recent work on AI accountability in judicial proceedings argues that predictive and generative systems should be understood as components of a broader socio-technical network that support, rather than replace, the situated human deliberation and responsibility that underpin judicial reasoning[30]. These concerns are especially relevant for Albania, where public trust is vital amid ongoing reforms. Górski et al. examine the role of XAI in regulated domains such as tax fraud detection, where transparency is crucial for procedural fairness[31]. Their findings indicate that XAI models enhance interpretability and secure accountability, offering valuable insights for Albania's judiciary. These concerns about transparency and public confidence are consistent with broader findings that trust in courts is strongly shaped by perceptions of procedural fairness, openness, and opportunities to contest decisions[32]. As Albania modernizes its judicial system, transparency in AI-driven decisions is essential to building public trust and maintaining integrity in legal processes.

Barysė and Sarel investigate public perceptions of AI in judicial decision-making, finding broad acceptance of AI for low-risk tasks like evidence gathering but significant skepticism regarding its use in consequential decisions such as verdicts. Legal professionals are particularly concerned about AI's fairness and reliability in these contexts[33]. The study advocates for a phased approach to AI integration that begins with low-risk tasks to build public confidence. Comparative research on courts and artificial intelligence indicates that many judiciaries currently confine AI to low-risk, workflow-oriented tools, while remaining cautious about outcome-shaping applications because concerns about transparency and accountability in adjudication are not yet resolved[34]. This approach is well suited to Albania's ongoing judicial reforms.

Schweitzer and Conrads assess the performance of AI models like ChatGPT-4 in resolving German business law cases, showing accuracy improvements but highlighting inconsistencies in complex legal scenarios[35]. Their findings emphasize the need for human oversight, a crucial factor

26. Ferhataj–Memaj–Sahatcija et al. 2025.
27. Ilin–Kelli 2024.
28. Szkalej–Senftleben 2024.
29. Engel–Linhardt–Schubert 2025.
30. Contini–Ontanu–Velicogna 2024.
31. Górski–Kuźniacki–Almada et al. 2025.
32. Wallace–Goodman Delahunty 2021.
33. Barysė–Sarel 2024.
34. Reiling 2020.
35. Schweitzer–Conrads 2025.

in Albania's judicial system, where robust oversight mechanisms are necessary to mitigate risks and build trust in AI-driven legal tools.

Governance frameworks are fundamental to building trust in AI systems. Di Porto et al. demonstrate how advanced NLP can enhance inclusivity and reduce bias in policymaking, offering a model for Albania's public engagement in AI governance[36]. Fernández-Llorca et al. address terminological inconsistencies in the EU's AI legislation, proposing methodologies for harmonizing technical and legal interpretations, insights that are crucial as Albania drafts governance policies aligned with international standards[37].

2.4. Actions undertaken in Europe

This section maps how Europe approaches AI in justice across three layers: European Union (EU), National Member, and Council of Europe.

At the EU level, regulation is binding via the AI Act's enforceable requirements. The EU Artificial Intelligence Act, enacted in 2024, is a cornerstone of this strategy. It classifies AI applications into four risk categories: unacceptable, high, limited, and minimal. High-risk AI systems, especially those in judicial contexts, are subject to stringent requirements for transparency, data quality, and human oversight to safeguard fundamental rights and societal values[38]. Its main strength is clarity of expectations for procurement and supervision. Its main limitation is operationalisation, since key details depend on secondary standards, conformity assessments, and local capacity. There is also a governance gap between generic product-safety controls and the constitutional sensitivities of courts, such as explainability that is meaningful for legal reasoning and not only for technical audits. The EU's commitment to fostering innovation in judicial systems is further exemplified by initiatives under Horizon Europe, which funds research into cutting-edge AI applications. Notable advancements include *LaCour!*, a multilingual legal corpus for enhancing legal research, and predictive tools for case prioritization, enabling courts to allocate resources more effectively[39].

EU Member states practice is experimenting mainly in low-risk workflow areas, including transcription, document search, case triage, and calendaring. The EU's binding framework channels innovation toward safe, workflow-oriented uses, and Estonia's e-Justice architecture exemplifies how such deployments can scale in practice while preserving explainability and human control. A prominent example is Estonia's e-Justice system, which has significantly improved judicial workflows. Estonia's e-Justice ecosystem shows how integration across institutions reduces friction. The *e-File* platform, an interconnected system linking courts, police, prosecutors, and correctional facilities, reduces administrative burdens and streamline case processing, thereby enhancing collaboration among stakeholders and improving efficiency[40]. Additionally, Estonia's *Salme*, an AI-powered speech recognition assistant, automates court hearing transcriptions, improving the speed and accuracy of documentation and freeing up resources for more complex judicial tasks[41]. The upside is tangible efficiency gains without displacing judicial judgment. The downside is fragmentation. Pilots vary in quality, evaluation methods are inconsistent, and results are rarely comparable or openly audited. Known risks, such as dataset bias, vendor lock-in, and legally adequate explainability, are often acknowledged but not yet addressed with systematic controls.

At the Council of Europe level, guidance consists of non-binding soft-law instruments that steer practice without creating legal duties. *European Ethical Charter on the Use of AI in Judicial Systems* (Council of Europe) offers comprehensive guidelines for the ethical deployment of AI in legal settings, emphasizing fairness, non-discrimina-

36. Di Porto–Fantozzi–Naldi–Rangone 2024.
37. Fernández-Llorca–Gómez–Sánchez–Mazzini 2025.
38. See *The AI Act Explorer*, in "artificialintelligenceact.eu", 2024; Farrell 2024.
39. Held–Habernal 2024; Laptev–Feyzrakhmanova 2024.
40. Gamito Cantero–Gentile 2023.
41. e-Estonia 2022.

tion, and the protection of fundamental rights[42]. A key component of ethical AI deployment is XAI, which enhances transparency and accountability by enabling users to understand and evaluate AI decisions. XAI is especially critical in consequential areas like judicial decision-making, where public trust hinges on the clarity and fairness of AI recommendations[43]. Its value lies in normative alignment across jurisdictions, including non-EU members. Its limits are its non-binding status and uneven uptake. Principles do not automatically become procurement clauses, testing protocols, or user training.

2.5. AI in Albania

Albania's judicial reforms, initiated in 2016, aim to modernize legal institutions, improve transparency, and restore public trust in alignment with EU standards[44]. These efforts present a critical opportunity to integrate AI to address systemic challenges such as case backlogs, inconsistent rulings, and low public confidence in the justice system. However, Albania's ICT adoption remains well below the European average, with serious gaps in key areas like Decision Support Systems and Digital Access to Justice[45]. According to the CEPEJ ICT Index (Fig. 2), Albania's Deployment Index (2.0) and Usage Index (1.6) are significantly lower than the Council of Europe (CoE) averages of Deployment Index (4.1) and Usage Index (3.3), highlighting critical gaps in ICT adoption[46]. These deficiencies are especially evident in Decision Support Systems (1.3) and Digital Access to Justice (1.4 for civil and administrative matters), underscoring the urgent need for AI-driven innovations to improve efficiency and accessibility. Predictive analytics could reduce the current average case disposition times, 2,272 days for civil cases, while AI tools for automated document processing and case management could streamline workflows and reduce administrative burdens.

The risk of algorithmic bias and data privacy issues is particularly concerning, given the historical biases embedded in legal and enforcement datasets[47]. Also, successful AI adoption in Albania must be accompanied by defensible ethical frameworks. Albania has now overhauled its privacy framework with Law No. 124/2024 "On Personal Data Protection"[48], which is aligned with the EU GDPR[49] regulation. On the ground, GDPR alignment strengthens Albania's system in five concrete ways: (1) limits on solely automated decisions with legal or similarly notable effects and the right to human intervention, to express a view, and to contest outputs[50]; (2) duties to provide meaningful information about the logic involved, significance, and envisaged consequences of automated processing[51]; (3) mandatory Data Protection Impact Assessments for high-risk processing in justice[52]; (4) "data protection by design and by default" that pushes vendors to build audit trails, access controls, and role-based explanations[53]; and (5) accountability and transparency obligations that formalise record-keeping, notices, and audits that courts

42. European Commission for the Efficiency of Justice 2018.
43. Engel–Linhardt–Schubert 2025.
44. European Commission 2024.
45. European Commission for the Efficiency of Justice 2024-a.
46. European Commission for the Efficiency of Justice 2024.
47. Barocas–Selbst 2016.
48. Parliament of Albania, Law No. 124/2024 "On Personal Data Protection" (*Ligj nr. 124/2024 Për mbrojtjen e të dhënave personale*).
49. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
50. Regulation (EU) 2016/679 (GDPR), Article 22(1)-(3).
51. Regulation (EU) 2016/679 (GDPR), Article 13(2)(f), Article 14(2)(g), and Article 15(1)(h).
52. Regulation (EU) 2016/679 (GDPR), Article 35.
53. Regulation (EU) 2016/679 (GDPR), Article 25(1)-(2).

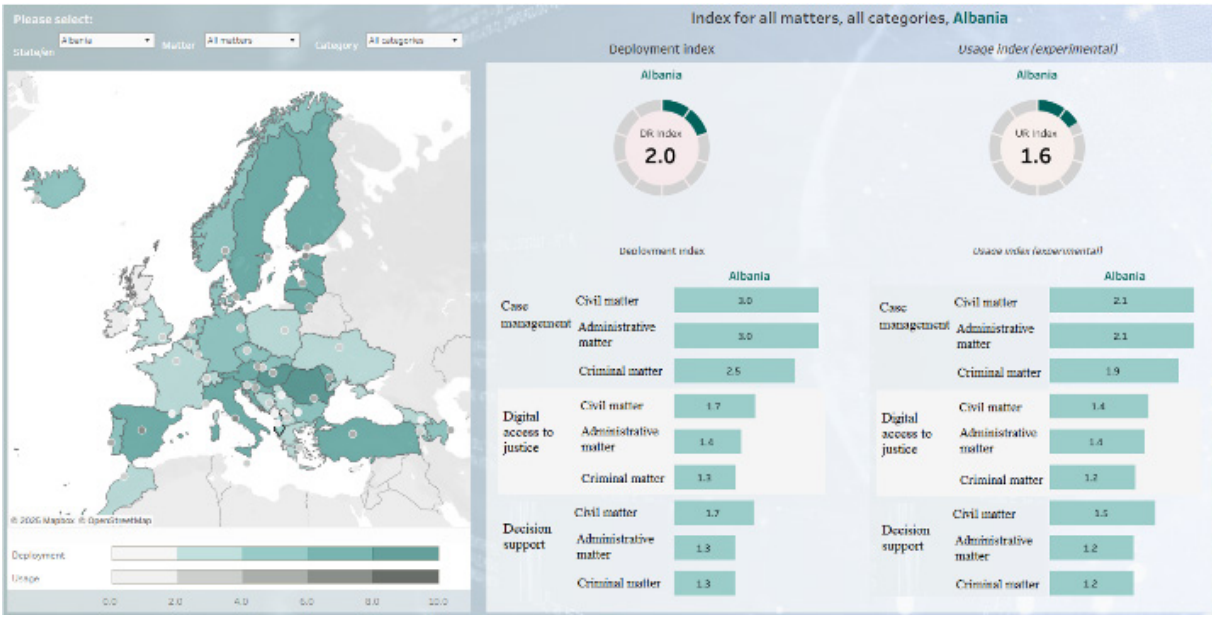

Fig. 2 — *CEPEJ ICT Index. By European Commission for the Efficiency of Justice (European Commission for the Efficiency of Justice, Report European judicial systems - CEPEJ Evaluation report - 2024 Evaluation cycle (2022 data), Council of Europe, 2024)*

and ministries can enforce through procurement[54]. These safeguards translate explainability and oversight into enforceable rights and procedures within Albanian institutions[55].

Also, AI integration requires substantial investment in human capital and public awareness. Albania's judicial professionals receive fewer ICT training sessions compared to the European average, limiting their ability to effectively adopt AI tools[56]. Targeted capacity-building programs focusing on AI literacy and ethical considerations, combined with public awareness campaigns, are essential for building support for AI within the judiciary. Given Albania's limited judicial budget (€15.8 per capita compared to €85.4 in the CoE)[57] AI solutions must be cost-effective and scalable. By addressing these challenges, Albania can leverage AI to modernize its judiciary, increase efficiency, and align with EU standards, while ensuring transparency, fairness, and accountability. This article recommends Estonia's e-Justice system as the most suitable model for Albania, particularly its *e-File* platform and AI-powered tools such as Salme for court transcription[58].

Guided by the research objectives and gaps identified in the literature, this study proposes the following hypotheses:

- H1: There is a significant positive correlation between students' perceptions of AI's potential to enhance judicial efficiency and their support for its application in non-critical functions (e.g., case management, document automation, preliminary evidence reviews) ($\alpha = 0.05$).
- H2: Higher perceived transparency in AI decision-making positively influences students' trust in their application for high-stakes judicial decisions (e.g., sentencing and parole recommendations) ($\alpha = 0.05$).
- H3: Students with higher ethical literacy regarding AI's societal implications are more likely to support the implementation of robust governance frameworks (e.g., AI ethics, transparency

54. Regulation (EU) 2016/679 (GDPR), Article 5(1)(a), 5(2), Article 12, Article 24, and Article 30.
55. Parliament of Albania, Law No. 124/2024 "On Personal Data Protection" (*Ligj nr. 124/2024 Për mbrojtjen e të dhënave personale*).
56. European Commission for the Efficiency of Justice 2024.
57. European Commission 2024.
58. Gamito Cantero–Gentile 2023; e-Estonia 2022.

policies, and regulatory oversight) to ensure fairness, accountability, and transparency in AI systems in judicial decision-making (α = 0.05).

3. Methodology

This research employs a quantitative approach within the positivist framework, analysing university students' perceptions of AI in the judicial sector. Set against the backdrop of Albania's ongoing judicial reforms and AI adoption, it provides a distinct perspective on how technological innovation intersects with legal transformation. This study evaluates students' views on the potential advantages and challenges of AI in judicial processes, while also addressing their concerns about the ethical, social, and operational impacts of AI integration.

3.1. Participants

The target population consists of Albanian university students from law, information technology (IT), and computer engineering disciplines. These students were selected due to their potential future roles as practitioners, policymakers, and technologists shaping AI's integration into the legal sector. Their insights are essential for gauging societal readiness for adoption of AI in judicial systems. A total of 340 students participated, providing a diverse sample. Participants were predominantly aged 20-24 years, with 53% female and 47% male. The academic distribution was: 40% law, 35% IT, and 25% computer engineering. Students were recruited through university networks and social media. Eligibility was screened via a questionnaire, and anonymized identifiers make sure data confidentiality.

3.2. Instrument Design

A structured questionnaire was developed to measure students' perceptions, attitudes, and ethical concerns about AI in judicial systems. The questionnaire was designed based on a thorough literature review to ensure validity and reliability[59]. Participants received brief, plain-language definitions before beginning the survey[60]. "Efficiency" was presented as outputs relative to resources, and "timeliness" referred to duration and backlogs. "Consistency" was introduced as the principle that like cases should be treated alike, with procedures and decisions applied coherently and predictably. In line with the EU Ethics Guidelines for Trustworthy AI, "fairness" was presented as the avoidance of unjustified bias and discrimination, ensuring equal treatment of individuals and groups. "Transparency" was described as the explainability, traceability, and communication of how AI tools operate in judicial processes, whereas "accountability" referred to the auditability of these tools, the minimisation and reporting of negative impacts, the management of trade-offs, and the availability of mechanisms for redress[61].

Questionnaire Structure:

- Demographics: Information on age, gender, and academic discipline.
- Knowledge and Exposure: Multiple-choice questions assessed familiarity with AI technologies and their judicial applications.
- Perceptions and attitudes (5-point Likert): judicial efficiency, transparency, accountability and human oversight, fairness, ethical concerns, trust in AI for high-stakes decisions, support for AI in non-critical court functions, and support for governance/regulatory frameworks.

The internal consistency of the questionnaire was assessed using Cronbach's alpha, yielding a value of 0.945, indicating high reliability and confirming the robustness of the instrument for this study (Tab. 1).

Estimate	Cronbach's α
Point estimate	0.945

Tab. 1 — *Frequentist Scale Reliability Statistics*

59. Dakalbab–Talib–Waraga et al. 2022; Simmons 2018; Perrot 2017.
60. European Commission for the Efficiency of Justice 2024; High-Level Expert Group on Artificial Intelligence 2019.
61. *Ibidem.*

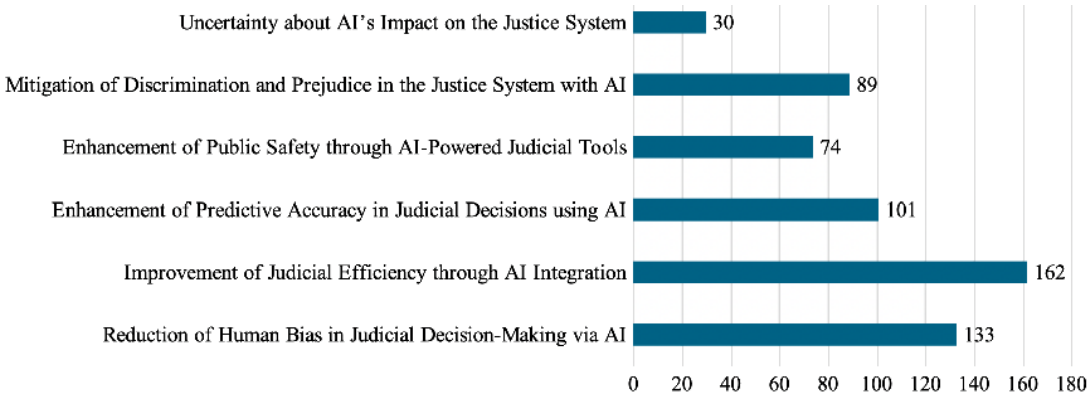

Fig. 3 — *Perceived Benefits of AI in the Justice System*

3.3. Data Collection and Analysis

Data were collected online between June and October 2024, ensuring accessibility, anonymity, and flexibility across institutions. Participants were fully informed about the study's aims, voluntary participation, and their right to withdraw at any point. Data were anonymized to safeguard confidentiality, with identifiable information excluded during analysis. Quantitative data analysis was performed using JASP 0.19.1.0. Descriptive Statistics summarized students' perceptions of AI's potential in enhancing judicial efficiency, fairness, transparency, and addressing ethical concerns. Spearman's Rank Correlation was used to explore relationships between students' perceptions and their attitudes toward AI integration in judicial processes[62]. This non-parametric method was appropriate due to the ordinal nature of the Likert scale data and its ability to detect monotonic relationships. Spearman's rank is particularly suitable for analyzing non-normally distributed data, as it does not rely on the assumption of normality. Statistical significance was set at $\alpha = 0.05$ (Type I error rate), with a 95% confidence interval.

4. Results

4.1. How do students perceive AI's potential to impact efficiency, fairness, and transparency in the justice system?

Table 2 (N = 340) reports item means (1–5) by discipline. Among IT/Computer Engineering (IT/CE) students, the highest mean is for transformative potential (3.578), followed by the ability to solve complex legal challenges (3.377), impartiality (2.966), and the enhancement of judicial efficiency (2.686). Law students show the same rank order: transformative potential (3.353), complex legal challenges (3.199), impartiality (3.11), and the enhancement of judicial efficiency (2.846). Between groups, IT/CE means are higher for transformative potential (+0.225) and complex challenges (+0.178), whereas Law means are higher for efficiency (+0.16) and impartiality (+0.144). This pattern aligns with the cohorts' training profiles, with IT/CE students emphasising innovation and analytic capability and Law students placing slightly more weight on workflow improvements and impartiality.

A deeper examination of the perceived benefits of AI in the justice system (Fig. 3) reveals that the most recognized benefit is the enhancement of judicial efficiency through AI integration, with 162 responses. The second most prominent benefit is the belief that AI can reduce human bias in judicial decision-making (133 responses). Students primarily associate AI with improving the efficiency and consistency of judicial processes. This article interprets "consistency of judicial processes" as the principle that like cases should be treated alike, and that decisions and procedures should be applied in a coherent, uniform, and predictable manner. In the students' responses, this concept appears to operate at two levels. At the systemic level, stu-

62. Lovie 1995.

Statement	Valid	Mean		Coefficient of variation	Minimum	Maximum
		IT/ Computer Engineering (204)	Law (136)			
AI's Potential to Enhance Judicial Efficiency	340	2.686	2.846	0.386	1	5
AI's Transformative Potential for the Justice System	340	3.578	3.353	0.344	1	5
AI's Ability to Solve Complex Legal Challenges	340	3.377	3.199	0.337	1	5
Perceptions of AI's Impartiality in Judicial Decision-Making	340	2.966	3.11	0.364	1	5

Tab. 2 — *Students' Perceptions on AI's Impact on the Justice System*

Statement	Valid	Mean		Coefficient of variation	Minimum	Maximum
		IT/ Computer Engineering (204)	Law (136)			
Concerns About the Negative Impacts of AI (Job Displacement, Privacy Violations, and Bias)	340	3.127	3.029	0.371	1	5
Ethical Implications of AI Use (Bias, Privacy, and Justice)	340	2.843	2.89	0.358	1	5
Impact of Growing Concerns Over Data Privacy and Security on the IT Industry	340	3.304	3.301	0.327	1	5
Concerns About Potential Biases in AI Algorithms Used in the Justice System	340	2.887	2.89	0.349	1	5
Risks of Unintended Consequences from AI, such as Hacking or Manipulation	340	3.186	3.162	0.339	1	5

Tab. 3 — *Students' Concerns Regarding AI's Ethical and Societal Impacts in the Justice System*

dents' responses reflect a strong desire to reduce unexplained differences in the outcomes of comparable cases. At the level of AI tools, it expresses an expectation that algorithms might reduce randomness or arbitrariness in decision support by applying the same criteria consistently over time. Other perceived benefits included improvements in the accuracy of case-outcome predictions and potential gains in public safety from AI-enabled tools, although these were mentioned less often.

Thirty students reported uncertainty regarding the broader role and impact of AI within the justice system. This points to the need for enhanced education and awareness about AI's capabilities and limitations, particularly for future legal professionals who must navigate the ethical complexities of AI integration into judicial decision-making. While many students regard AI as a promising instrument for legal reform, they also expressed concern about its ability to replicate human judgment and to meaningfully address enduring issues such as bias and fairness. These results emphasize the importance of continued research and education on the ethical implications of AI, as well as its potential to drive transparency and fairness in judicial decision-making.

4.2. What concerns do students have regarding algorithmic bias, ethical implications, and societal impacts of AI in judicial decision-making?

The findings, as shown in Table 3 and Figure 3, reveal students' key concerns about the ethical, algorithmic, and societal implications of AI in judicial decision-making. Generally, students express concerns across different programs to a moderate extent. The most prominent point of consensus amongst the students is that of data privacy and security, which is similar in both groups (IT/CE 3.304; Law 3.301) and exhibits the least variation (coefficient of variation 0.327). Students also keep articulating their concerns regarding the possible negative outcomes like hacking or manipulation (IT/CE 3.186; Law 3.162). The negative impact composite including job-loss, violation of privacy, and unfairness, is just over the midpoint (IT/CE 3.127; Law 3.029). When the worries are expressed in terms of biases in algorithms or ethical implications, the scores are centered around the middle of the scale (bias: IT/CE 2.887, Law 2.89; ethics: IT/CE 2.843, Law 2.89). It suggests that the students trust the technology under certain conditions. Many of them do not mind the use of AI in the courts if very effective protective measures are implemented. There is not much difference between the two fields of study. IT/CE students score only 0.098 higher in terms of negative impacts and 0.024 in unintended-consequence risks. Law students, on the other hand, score 0.047 and 0.003 higher in terms of ethics and bias respectively. The highest variability is noted for the negative-impacts composite (coefficient of variation 0.371), signifying that there are more widely spread opinions about the larger society's consequences of AI. All the factors point to a single interpretation. Privacy and security measures are the most common priority of the public, operational risks follow close behind, and concerns about bias and ethics are moderate, thus indicating the importance of privacy-by-design, strong security and visible oversight in making AI credible for the judiciary.

Figure 4 shows four main potential drawbacks of using AI in the justice system in the following order. First, the reduction of human oversight in decision making is the most common with 35% of the interviewed. Second, the decreased accountability and transparency with 26%, the familiar "black box"[63] problem. Third, the reinforcement of existing biases in data with 23%, and fourth, the perpetuation of systemic injustices with 16%. The ranking is the same across disciplines. IT and Computer Engineering students select each risk more often than Law students: oversight reduction 102 vs 61, accountability and transparency 78 vs 44, bias reinforcement 65 vs 43, systemic injustices 44 vs 33. These results point to three priorities: strong human oversight, clear explainability with audit trails, and active bias detection and mitigation.

4.3. How do students evaluate the role of transparency and accountability in fostering trust in AI-driven judicial systems?

The survey results, presented in Table 4 and visualized in Figures 5 and 6, reveal students' views on the importance of transparency, accountability, and human oversight in building trust in AI-driven judicial systems. Students are cautiously open to AI in the courts. Human oversight is the clearest priority overall (Law 3.426; IT/CE 3.299). Transparency of AI algorithms in the justice system is also rated highly, especially by law students, who assign it an average score of 3.404, compared to 3.088 for IT/CE. Students also want humans to keep the final say in AI-informed decisions (Law

63. Laptev–Feyzrakhmanova 2024.

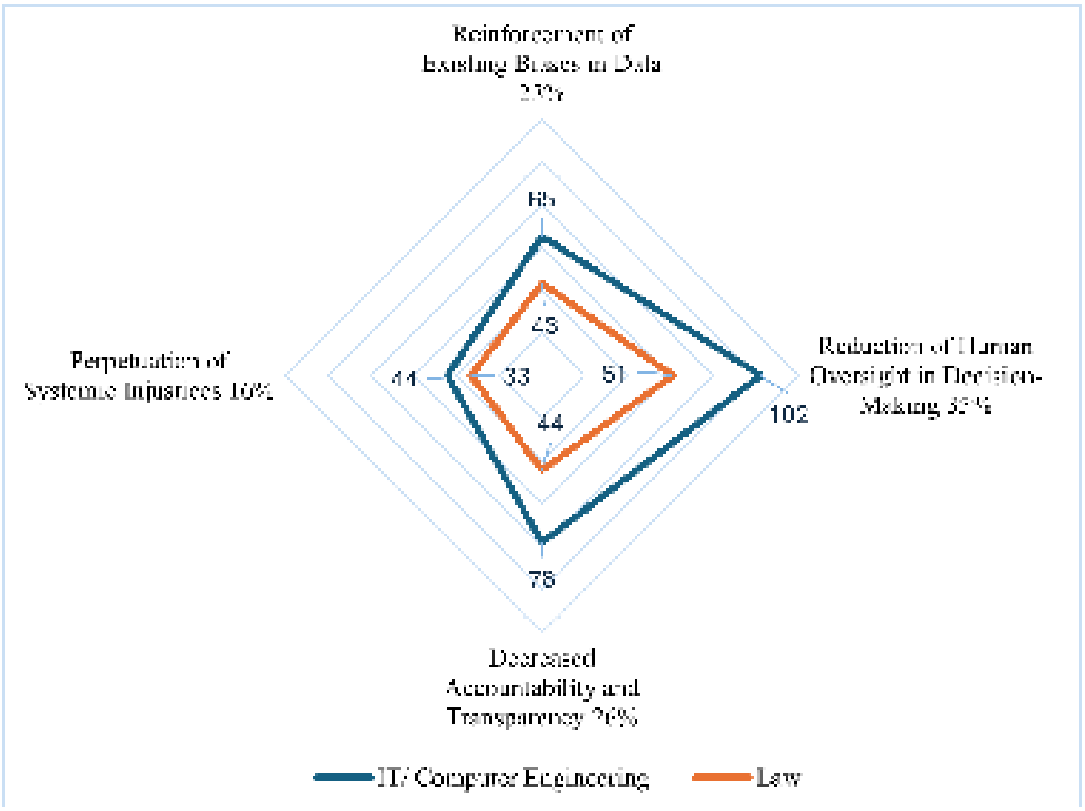

Fig. 4 — *Potential Drawbacks of Using AI in the Justice System*

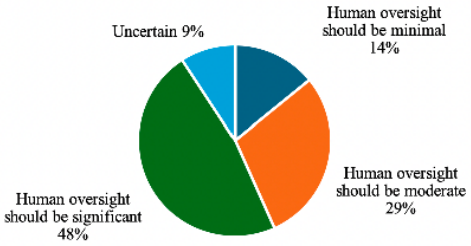

Fig. 5 — *The Role of Humans in AI Systems within the Justice System*

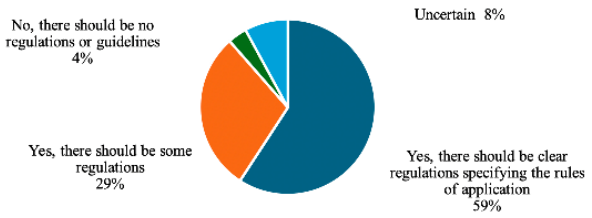

Fig. 6 — *Regulations for AI in Justice*

3.221; IT/CE 3.176) and they see value in AI training for justice professionals (Law 3.051; IT/CE 2.98). For the item on "transparency in AI systems", IT/CE students report slightly higher mean scores than law students (3.078 vs 3.007). Trust sits near the midpoint of the scale for both groups (IT/CE 2.897; Law 2.875), and views of accuracy are similarly moderate (IT/CE 2.941; Law 2.897). Support for using AI in high-stakes judicial decisions sits below the midpoint in both groups (IT/CE 2.583; Law 2.64), and this item shows the widest relative dispersion (coefficient of variation 0.429), indicating mixed views.

Differences by discipline are modest. Law students lean more strongly toward algorithmic transparency and oversight, while IT/CE students rate system-level transparency and perceived accuracy slightly higher. Taken together, the numbers point to three conditions for trust: make AI reasoning auditable, keep humans in charge at decision points, and equip legal professionals with the skills to question and contest AI outputs.

A notable majority of students (48%) demand that a human supervisor should be always present, which indicates that there is almost a universal agreement that judges should be assisted by AI and

Statement	Valid	Mean		Coefficient of variation	Minimum	Maximum
		IT/ Computer Engineering (204)	Law (136)			
Trust in AI-Driven Decisions	340	2.897	2.875	0.313	1	5
Transparency in AI Systems	340	3.078	3.007	0.31	1	5
Accuracy and Reliability of AI Predictions	340	2.941	2.897	0.332	1	5
Transparency of AI Algorithms in the Justice System	340	3.088	3.404	0.357	1	5
Human Oversight in AI Decision-Making	340	3.299	3.426	0.352	1	5
AI in High-Stakes Judicial Decisions	340	2.583	2.64	0.429	1	5
Human's Final Role in AI-Informed Legal Decisions	340	3.176	3.221	0.366	1	5
AI Knowledge Among Justice Professionals	340	2.98	3.051	0.355	1	5

Tab. 4 — *Role of Transparency, Accountability, and Human Oversight in AI-Driven Judicial Systems*

not replaced (Fig. 5). The next group of 29% supports the idea of moderate supervision, meaning that AI could take over the mundane or less critical tasks while humans would be in charge of important decisions. The least preferred option (14%) is the one with minimal supervision, where the use of clear guidelines and monitoring would allow certain operations to be performed independently. All in all, the trend suggests a human-in-the-loop approach, mainly for very important decisions.

A majority of the student population (59%) supports the implementation of definite and binding rules concerning AI usage in the legal system (Fig. 6). Just 29% are for the regulation but favor the flexible and adaptive guidelines. There are 4% who do not think that regulation is necessary at all and 8% who have no opinion. The general trend indicates a great backing for the created regulations that would limit the use of AI to legal areas, reduce the probability of the emergence of ethical issues, and at the same time, give a space for responsible innovation.

4.4. H1: There is a significant positive correlation between students' perceptions of AI's potential to enhance judicial efficiency and their support for its application in non-critical functions (e.g., case management, document automation, preliminary evidence reviews) ($\alpha = 0.05$)

The results of the Spearman's rank correlation analysis support Hypothesis 1 (H1), revealing a small to moderate positive correlation between students' perceptions of AI's potential to improve judicial efficiency in Albania's judiciary and their level of support for its application in non-critical functions such as case management, document automation, and preliminary evidence review (Tab. 5). The Spearman's rho of 0.277 indicates that as students perceive AI to be more effective in enhancing judicial efficiency, they are more likely to support its use in routine judicial tasks. This correlation is statistically significant, with a p-value of < 0.001. These findings suggest that students who view AI positively in terms of judicial efficiency are more inclined to accept its application in administrative functions that do not require subjective hu-

Variable		Students' Perceptions of AI's Potential to Enhance Judicial Efficiency	Support for AI's Application in Non-Critical Functions
Students' Perceptions of AI's Potential to Enhance Judicial Efficiency	n	—	
	Spearman's rho	—	
	p-value	—	
Support for AI's Application in Non-Critical Functions	n	340	—
	Spearman's rho	0.277***	—
	p-value	< .001	—

* p < .05, ** p < .01, *** p < .001

Tab. 5 — *Spearman's Correlation Between Perceived AI Efficiency and Support for Non-Critical Judicial Applications*

man judgment. Also, the moderate strength of the correlation (0.277) also implies that other factors, such as ethical concerns, trust in AI, and awareness of its limitations, may influence students' attitudes toward AI in the judicial system[64].

These results have important implications for policymakers and AI developers, highlighting the need to demonstrate AI's potential to enhance judicial efficiency to build broader acceptance, particularly in non-critical functions[65].

4.5. H2: Higher perceived transparency in AI decision-making positively influences students' trust in their application for high-stakes judicial decisions (e.g., sentencing and parole recommendations) ($\alpha = 0.05$)

The results of the Spearman's rank correlation analysis support Hypothesis 2 (H2), revealing a small to moderate positive correlation between students' perceptions of transparency in AI decision-making and their trust in their application for high-stakes judicial decisions, such as sentencing and parole recommendations. The Spearman's rho of 0.262 indicates that as students perceive AI decision-making processes to be more transparent, they are more likely to trust AI in sensitive legal contexts. This correlation is statistically significant (p-value < 0.001), emphasizing the importance of transparency as a critical factor in building trust in AI applications within the judicial system[66].

These findings underscore the essential role of explainability and clarity in AI systems, particularly in consequential judicial decisions where errors or perceived biases can have serious personal and societal consequences[67]. Transparency in AI decision-making is crucial for maintaining public confidence, especially in judicial contexts where the stakes are high. This supports the argument that transparent AI systems are vital for ensuring fairness and accountability in judicial decisions, in line with ethical principles of justice[68]. Additionally, these findings suggest that enhancing transparency in AI decision-making could be an effective strategy to build trust and facilitate the broader adoption of AI in high-stakes judicial functions. These results contribute to ongoing discussions about the ethical deployment of AI in the justice system, highlighting the need for clear, explainable

64. Laptev–Feyzrakhmanova 2024.
65. Engel–Linhardt–Schubert 2025; Simmons 2018.
66. Engel–Linhardt–Schubert 2025; Barysė–Sarel 2024.
67. Di Porto–Fantozzi–Naldi–Rangone 2024; Laptev–Feyzrakhmanova 2024.
68. Simmons 2018.

Variable		Perception of transparency in AI decision-making	Trust in AI for high-stakes judicial decisions
Perception of transparency in AI decision-making	n	—	
	Spearman's rho	—	
	p-value	—	
Trust in AI for high-stakes judicial decisions	n	340	—
	Spearman's rho	0.262***	—
	p-value	< .001	—

* p < .05, ** p < .01, *** p < .001

Tab. 6 — *Spearman's Correlation Between Perceived AI Transparency and Trust in High-Stakes Judicial Decisions*

AI models to secure ethical and fair decision-making[69] (Tab. 6).

4.6. H3: Students with higher ethical literacy regarding AI's societal implications are more likely to support the implementation of robust governance frameworks (e.g., AI ethics, transparency policies, and regulatory oversight) to ensure fairness, accountability, and transparency in AI systems in judicial decision-making (α = 0.05)

The results of the Spearman's rank correlation analysis provide support for Hypothesis 3 (H3), revealing a moderate-to-strong positive correlation between students' ethical literacy regarding AI's societal implications and their support for robust governance frameworks aimed at ensuring fairness, accountability, and transparency in AI systems used in judicial decision-making (Tab. 7). The Spearman's rho of 0.523 ($p < 0.001$) indicates a statistically significant correlation, emphasizing the critical role that ethical education plays in shaping students' attitudes toward responsible AI governance.

As students' awareness of AI's societal risks, such as algorithmic bias, privacy violations, and discrimination grows, so does their support for comprehensive regulatory oversight and transparent AI frameworks. This aligns with the broader literature, which shows the importance of embedding ethical principles into the design and deployment of AI systems, particularly in consequential sectors like the judicial system[70]. These findings highlight the need to incorporate ethical literacy into educational curricula for future legal and technology professionals. By building a deeper understanding of AI's broader societal implications, such education equips students to engage proactively with policies that promote fairness and accountability in AI-driven decision-making. This proactive engagement is essential for ensuring that AI is used ethically, particularly in judicial contexts, where AI-driven decisions can significantly impact individuals' rights and liberties[71].

Also, the findings reinforce the importance of ethical oversight and human involvement in AI-driven judicial decisions, a central component of the AI-Driven Justice System Framework proposed in this study. This framework advocates for a balanced approach, where human judgment remains integral, especially in sensitive judicial decisions. As AI systems are increasingly integrated into judicial processes, human decision-makers play a crucial role in ensuring ethical compliance and transparency, mitigating the risks associated

69. Górski–Kuźniacki–Almada et al. 2025; Schweitzer–Conrads 2025.

70. Bex 2025.

71. Gless 2023; Perrot 2017.

Variable		Ethical literacy regarding AI's societal implications	Support for the implementation of robust governance frameworks
Ethical literacy regarding AI's societal implications	n	—	
	Spearman's rho	—	
	p-value	—	
Support for the implementation of robust governance frameworks	n	340	—
	Spearman's rho	0.523***	—
	p-value	< .001	—

Source: Author creation

* p < .05, ** p < .01, *** p < .001

Tab. 7 — *Spearman's Correlation Between Ethical AI Literacy and Support for Judicial AI Governance Frameworks*

with unchecked AI deployment[72]. These results underscore societal concerns and the need for comprehensive, transparent AI governance frameworks to regulate AI in justice.

5. The AI-Driven Justice System Framework

This study explores the integration of AI into transitional judicial systems, with an emphasis on enhancing efficiency, fairness, transparency, and ethical governance. The data suggests cautious optimism regarding AI's potential to improve judicial efficiency, optimize workflows, and address complex legal challenges. Also, concerns about algorithmic bias, data privacy, and the need for human oversight remain serious. These insights underscore the importance of a structured framework for the responsible deployment of AI in the justice system. Accordingly, we introduce the AI-Driven Justice System Framework, designed to address these challenges while ensuring ethical, transparent, and accountable use of AI. The AI-Driven Justice System Framework combines AI's capabilities with ethical governance and public trust-building. It consists of four key components derived from the study's findings:

AI Judicial Workflow: AI can enhance judicial efficiency by automating routine tasks, such as case prioritization, document processing, and legal research, thereby reducing administrative burdens and enabling judges to focus on more complex cases. While students recognize AI's efficiency for non-critical tasks, concerns persist regarding its integration into high-stakes judicial decisions.

Transparent & Explainable AI (XAI): The framework makes clear the need for transparency in AI decision-making, especially in critical areas such as sentencing and parole. XAI safeguards that decisions made by AI systems are understandable, auditable, and accountable, building public trust.

Ethical Governance & Human Oversight: Ethical concerns, particularly algorithmic bias and accountability, are central to this study. The framework prioritizes continuous bias monitoring, regular audits, and human oversight, ensuring that judges retain final authority over decisions and minimize the risk of AI perpetuating biases.

72. Laptev–Feyzrakhmanova 2024.

Public Engagement & Trust: Building and maintaining public trust is crucial for AI's integration into the justice system. The framework encourages the development of transparency portals and educational initiatives that inform citizens about AI's role in judicial processes, promoting informed public engagement.

The AI-Driven Justice System Framework will provide a comprehensive, actionable model for integrating AI into judicial systems, emphasizing efficiency, transparency, ethical governance, and public engagement. By addressing concerns and building trust, this framework will ensure that AI-driven judicial reforms are aligned with societal values and serve the greater good.

6. Conclusion

This paper studies how future legal and technology professionals in Albania perceive the ethical integration of AI into judicial systems, at a moment when the judiciary is still at a pre-adoption stage. Drawing on survey data from 340 law, IT, and computer engineering students in Albania, it examined how they evaluate AI's potential for efficiency, fairness, and transparency; what concerns they hold about its ethical and societal implications; and how transparency and accountability shape their trust in AI-driven judicial systems. The results point to a pattern of cautious optimism: students see AI as a promising tool for improving judicial workflows and addressing complex legal problems, but only under conditions of strong human oversight, rigorous governance, and meaningful transparency.

Across disciplines, three clusters of concern emerge from the data. First, privacy and data security are consistently rated as top priorities, with students wary of hacking, manipulation, and misuse of sensitive information. Second, there is sustained unease about bias, unfairness, and the risk that AI might reproduce or amplify existing structural inequalities. Third, many respondents worry that opaque "black box" tools could weaken accountability and erode public trust if introduced without visible safeguards. At the same time, the data shows that students are more supportive of AI where they perceive higher levels of transparency and oversight, and where ethical implications are openly acknowledged and governed. Ethical literacy appears to play a particularly important role: those who are more aware of AI's societal risks are also more inclined to endorse strong regulatory and governance frameworks, rather than rejecting AI outright.

These insights are synthesized in the AI-Driven Justice System Framework proposed by this article. The framework translates students' preferences into four complementary pillars: workflow-oriented AI to relieve administrative burdens and address backlogs; transparent and explainable systems in any context where AI influences legal outcomes; robust ethical governance and human oversight, including bias monitoring, audits, and a clear human final say; and public engagement strategies that foster understanding, scrutiny, and trust. For a transitional judiciary such as Albania's, this framework provides a structured pathway for aligning AI adoption with European regulatory developments, and national expectations of fairness and accountability.

Future research should monitor changes over time, compare cross-national experiences, and evaluate specific pilot projects through published audits and user-centered testing of explanations. While AI can reduce delays, improve consistency, and allow legal professionals to focus on judgment, it should not replace that judgment. A measured, transparent, and human-guided approach offers the most credible route to real efficiency gains while safeguarding rights and maintaining public trust.

6.1. Recommendations

Grounded in the study's evidence, several analytically driven recommendations emerge for responsible judicial adoption of AI. First, AI should be deployed primarily as an assistive mechanism for non-critical, workflow-oriented tasks, while all consequential determinations remain under robust human-in-the-loop review. This division preserves judicial discretion and ensures that machine outputs support, rather than substitute, legal judgment. Second, systems must meet stringent transparency and explainability standards. This includes providing case-level rationales that allow judges and lawyers to understand and contest outputs, publicly disclosing when and where AI is used, and maintaining detailed system-level documentation covering data inputs, model limitations, and update histories. These measures create trace-

ability and make system behaviour intelligible to both professionals and the public.

Institutionalised governance structures are essential. Courts should integrate pre-deployment impact assessments, define scheduled bias and accuracy audits, and maintain comprehensive audit logs that record system recommendations and human overrides. A designated AI governance lead or office should coordinate compliance, monitoring, and inter-institutional communication. Privacy and data-protection responsibilities should follow established principles such as data minimisation, precise retention schedules, and secure, auditable access controls. These controls ensure that efficiency gains do not compromise fundamental rights.

To strengthen public trust, judicial institutions should establish a dedicated transparency portal that provides plain-language information on AI tools, their purposes, datasets, and safeguards. Regular publication of performance metrics, complaint data, and appeal outcomes linked to AI use can further reinforce accountability. Ethical and technical literacy should also be embedded through continuous training for judges, clerks, and practitioners, coupled with curricular inclusion in both law and computer-science programs. This supports a workforce capable of critically evaluating and responsibly supervising AI systems.

Finally, adoption should follow a measured pilot-to-scale pathway. Expansion should occur only when empirical indicators such as reduced time to disposition, backlog reduction, error and override rates, disparate-impact measures, satisfaction with explanations, and stable staff uptake demonstrate clear and sustained benefit. This evidence-based progression limits risk while ensuring that AI contributes meaningfully to efficiency, fairness, and institutional legitimacy.

References

A.D. Reiling (2020), *Courts and artificial intelligence*, in "International Journal for Court Administration", vol. 11, 2020, n. 2

S. Barocas, A.D. Selbst (2016), *Big Data's Disparate Impact*, in "California Law Review", vol. 104, 2016, n. 3

D. Barysė, R. Sarel (2024), *Algorithms in the court: does it matter which part of the judicial decision-making is automated?*, in "Artificial Intelligence and Law", vol. 32, 2024, n. 1

F. Bex (2025), *AI, Law and beyond. A transdisciplinary ecosystem for the future of AI & Law,* in "Artificial Intelligence and Law", vol. 33, 2025

F. Contini, A. Minissale, S. Bergman Blix (2024), *Artificial intelligence and real decisions: predictive systems and generative AI vs. emotive-cognitive legal deliberations*, in "Frontiers in Sociology", vol. 9, 2024

F. Contini, E.A. Ontanu, M. Velicogna (2024), *AI Accountability in Judicial Proceedings: An Actor-Network Approach*, in "Laws", vol. 13, 2024, n. 6

F. Dakalbab, M.A. Talib, O.A. Waraga et al. (2022), *Artificial intelligence & crime prediction: A systematic literature review*, in "Social Sciences & Humanities Open", vol. 6, 2022, n. 1

F. Di Porto, P. Fantozzi, M. Naldi, N. Rangone (2024), *Mining EU consultations through AI*, in "Artificial Intelligence and Law", 2024

e-Estonia (2022), *Introducing Salme, Estonian courts' speech recognition assistant*, in e-"estonia.com", 26 January 2022

C. Engel, L. Linhardt, M. Schubert (2025), *Code is law: how COMPAS affects the way the judiciary handles the risk of recidivism*, in "Artificial Intelligence and Law", vol. 33, 2025

European Commission (2024), *Rule of Law Report: Country Chapter on the Rule of Law Situation in Albania*, SWD(2024) 828, 2024

European Commission for the Efficiency of Justice (2024), *Report European judicial systems - CEPEJ Evaluation report - 2024 Evaluation cycle (2022 data)*, Council of Europe, 2024

European Commission for the Efficiency of Justice (2024-a), *CEPEJ ICT Index*, 2024

European Commission for the Efficiency of Justice (2018), *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, Council of Europe, 2018

J. Farrell (2024), *An introduction to Codes of Practice for the AI Act*, 3 July 2024, in EU Artificial Intelligence Act

A. Ferhataj, F. Memaj, R. Sahatcija et al. (2025), *Ethical concerns in AI development: analyzing students' perspectives on robotics and society*, in "Journal of Information, Communication and Ethics in Society", vol. 23, 2025, n.2

D. Fernández-Llorca, E. Gómez, I. Sánchez, G. Mazzini (2025), *An interdisciplinary account of the terminological choices by EU policymakers ahead of the final agreement on the AI Act: AI system, general purpose AI system, foundation model, and generative AI*, in "Artificial Intelligence and Law", vol. 33, 2025

M. Gamito Cantero, G. Gentile (2023), *Algorithms, rule of law, and the future of justice - Implications in the Estonian justice system*, European University Institute, STG, Policy Brief, 2023/27, 2023

S. Gless (2023), *Could Robot Judges Believe? Epistemic Ambitions of the Criminal Trial as we approach the Digital Age: A Comment on Sarah Summers «Epistemic Ambitions of the Criminal Trial: Truth, Proof, and Rights»*, in "Quaestio Facti. Revista Internacional Sobre Razonamiento Probatorio", vol. 5, 2023

Ł. Górski, B. Kuźniacki, M. Almada et al. (2025), *Exploring explainable AI in the tax domain*, in "Artificial Intelligence and Law", vol. 33, 2025

L. Held, I. Habernal (2024), *LaCour!: enabling research on argumentation in hearings of the European Court of Human Rights*, in "Artificial Intelligence and Law", 2024

High-Level Expert Group on Artificial Intelligence (2019), *Ethics Guidelines for Trustworthy AI*, European Commission, 2019

I. Ilin, A. Kelli (2024), *Natural Language, Legal Hurdles: Navigating the Complexities in Natural Language Processing Development and Application*, in "Journal of the University of Latvia. Law", vol. 17, 2024

V. Laptev, D. Feyzrakhmanova (2024), *Application of Artificial Intelligence in Justice: Current Trends and Future Prospects*, in "Human-Centric Intelligent Systems", vol. 4, 2024, n. 3

J.-S. Lee (2025), *InstructPatentGPT: training patent language models to follow instructions with human feedback*, in "Artificial Intelligence and Law", vol. 33, 2025

A.D. Lovie (1995), *Who discovered Spearman's rank correlation?*, in "British Journal of Mathematical and Statistical Psychology", vol. 48, 1995, n. 2

P. Marshall (2022), *Scandal at the Post Office: The intersection of law, ethics and politics*, in "Digital Evidence and Electronic Signature Law Review", vol. 19, 2022

O. Metsker, E. Trofimov, G. Kopanitsa (2021), *Application of Machine Learning for E-justice*, in "Journal of Physics: Conference Series", vol. 1828, 2021

P.M. Nowotko (2021), *AI in judicial application of law and the right to a court*, in "Procedia Computer Science", vol. 192, 2021

P. Perrot (2017), *What about AI in criminal intelligence? From predictive policing to AI perspectives*, in "European Police Science and Research Bulletin", 2017

S. Schweitzer, M. Conrads (2025), *The digital transformation of jurisprudence: an evaluation of ChatGPT-4's applicability to solve cases in business law*, in "Artificial Intelligence and Law", vol. 33, 2025

R. Simmons (2018), *Big Data, Machine Judges, and the Legitimacy of the Criminal Justice System*, in "University of California Davis Law Review", vol. 52, 2018

K. Szkalej, M. Senftleben (2024), *Generative AI and Creative Commons Licences - The Application of Share Alike Obligations to Trained Models, Curated Datasets and AI Output*, in "Journal of Intellectual Property, Information Technology and Electronic Commerce Law", vol. 15, 2024, n. 3

A. Wallace, J. Goodman-Delahunty (2021), *Measuring trust and confidence in courts*, in "International Journal for Court Administration", vol. 12, 2021, n. 3

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0263 • articolo sottoposto a peer review • pubblicato in anteprima il 27 gen. 2026

Paolo Zuddas

Sul rapporto tra *human enhancement* e tutela della dignità: la dignità umana e sociale del lavoratore "aumentato"

Il contributo analizza il concetto di *human enhancement*, inteso come utilizzo di tecnologie biomediche su individui sani per finalità non terapeutiche, con l'obiettivo di migliorarne le prestazioni, l'aspetto o il benessere. Dopo aver chiarito la distinzione tra interventi medici terapeutici e potenziativi, si evidenzia, da un lato, il ruolo centrale della finalità performativa e, dall'altro, il carattere tendenzialmente permanente degli interventi, quali caratteri distintivi delle pratiche in parola. L'indagine si rivolge quindi all'impiego delle tecniche di potenziamento in ambito lavorativo, evidenziando i rischi di lesione della dignità umana del lavoratore derivanti soprattutto dall'innesto di dispositivi potenzianti collegati alle Rete, ascrivibili all'ambito dell'"Internet of bodies", che espongono il lavoratore a forme di controllo configurabili propriamente in termini di reificazione. Si sottolinea, in conclusione, l'impatto del ricorso alle tecnologie in esame sulla pari dignità sociale dei lavoratori, derivante dalla capacità degli interventi di *enhancement* di dar luogo a significative disparità – anche in termini di valore sociale – tra lavoratori potenziati e non potenziati (e tra gli stessi lavoratori potenziati), suscettibili di generare nuove forme di discriminazione sociale.

Human enhancement – Lavoro – Dignità umana – Dignità sociale

On the relationship between human enhancement and the protection of dignity: The human and social dignity of the "enhanced" worker

This article analyses the concept of human enhancement, understood as the use of biomedical technologies on healthy individuals for non-therapeutic purposes, with the aim of improving their performance, looks or well-being. After clarifying the distinction between therapeutic and enhancement medical interventions, it highlights, on the one hand, the central role of performance and, on the other hand, the generally permanent nature of the interventions, as distinctive features of the practices in question. The investigation then turns to the use of enhancement techniques in the workplace, highlighting the risks of violation of the human dignity of workers, deriving above all from the implantation of enhancement devices connected to the Internet, attributable to the "Internet of bodies", which expose workers to forms of control that can be properly described in terms of reification. Finally, the impact of the use of the technologies in question on the equal social dignity of workers is emphasized, deriving from the ability of enhancement interventions to give rise to significant disparities – also in terms of social value – between enhanced and non-enhanced workers (and between enhanced workers themselves), which are likely to generate new forms of social discrimination.

Human enhancement – Work – Human dignity – Social dignity

L'Autore è professore ordinario di Diritto costituzionale e pubblico presso l'Università dell'Insubria

Il presente lavoro riproduce, con qualche modifica, il testo dell'intervento svolto alla VI Conferenza annuale ICON'S Italy, sul tema *Lo Stato* vis à vis *i poteri economici e privati nell'era digitale*, svoltosi a Cagliari il 3 e il 4 ottobre 2025

Sommario: 1. La nozione di *human enhancement*: strumenti, obiettivi, limiti. – 2. La dignità umana del lavoratore aumentato: gli interventi permanenti sul corpo del lavoratore tra alterazione morfologica e reificazione. – 3. La dignità sociale del lavoratore aumentato: il potenziamento come fonte di nuove forme di discriminazione sociale.

1. La nozione di *human enhancement*: strumenti, obiettivi, limiti

Tra le diverse definizioni che compaiono nei documenti, sia nazionali che sovranazionali, che affrontano il tema del potenziamento umano, una delle più articolate – e dunque in grado di cogliere con precisione ed efficacia le molteplici implicazioni della tematica – appare quella elaborata in seno al Consiglio d'Europa: "Human enhancement can be defined as the use of medical technology to improve the performance, looks, or well-being of healthy, normal individuals for non-medical purposes"[1].

La formula richiamata – che si intende proporre come punto di partenza per una prima riflessione sul tema – si mostra particolarmente utile anzitutto perché individua il tipo di tecnologia utilizzata: "the use of medical technology". La tecnologia medica – o biomedica per la precisione, ricomprendendo anche le biotecnologie (insieme alle specifiche applicazioni della farmacologia e delle scienze cognitive) – rappresenta infatti il fulcro delle *human enhancement technologies*. In realtà, l'ambito delle applicazioni tecnologiche è più vasto, e coinvolge anche la robotica, l'impiantistica, le nanotecnologie, la genomica, la stessa intelligenza artificiale: si parla di norma in questo caso di tecnologie GRIN, cioè Geno, Robo, Info, Nano-tecnologie[2]; ma il nucleo è costituito dalla tecnologia biomedica.

La vera novità rappresentata dallo *human enhancement*, tuttavia, non è ascrivibile all'utilizzo delle nuove tecnologie in campo medico. Da sempre la medicina si è avvalsa delle conoscenze scientifiche e delle tecnologie sviluppate in altri ambiti per realizzare i propri fini: in ogni epoca, le nuove tecnologie del tempo sono state impiegate di norma anche in ambito medico. Anzi, sovente è avvenuto il contrario: la necessità di curare le malattie ha dato un impulso allo sviluppo di nuovi strumenti tecnologici[3]. La vera novità consiste nell'obiettivo perseguito: l'utilizzo di tecnologie bio-mediche per fini non medici ("for non-medical purposes").

Ma la definizione del Consiglio d'Europa sul punto è ancora più netta: gli interventi di potenziamento sono tali quando si rivolgono a persone "healty" e "normal" (in salute e normali).

Si evocano qui due condizioni che richiedono tuttavia di essere opportunamente modulate in relazione al contesto. In particolare, il significato dell'espressione "healty" va decisamente circoscritto: per individuo in salute deve intendersi, nella prospettiva in esame, una persona priva di quelle specifiche

1. La definizione compare in Rathenau Instituut 2014; si tratta del rapporto predisposto dal Rathenau Instituut dell'Aia nel 2014 per il Comitato per la Bioetica del Consiglio d'Europa (cfr. par. 4.4, p. 22). Il Rapporto affronta il tema delle tecnologie NBIC (nanotecnologie, biotecnologie, tecnologie dell'informazione e cognitive), che svolgono un ruolo fondamentale – insieme alla tecnologia medica, centrale in questo contesto – nello sviluppo delle pratiche di *human enhancement*.
2. Cfr. in tema Domenella 2023, p. 2; v. anche Palmerini 2024, p. 165.
3. Il settore medico insieme a quello militare hanno infatti rappresentato storicamente i settori c.d. "sentinella", nei quali si sono sviluppate per prime le nuove tecnologie (cfr. Maio 2020, p. 516).

patologie connesse all'intervento di *enhancement*; l'innesto, ad esempio, di un impianto neuronale su un soggetto paraplegico (volendo rievocare uno dei casi più noti di applicazione delle tecnologie in parola)[4] non costituisce propriamente un intervento di *enhancement*, in quanto, in quella circostanza, l'intervento medico viene realizzato per perseguire – almeno in prevalenza – finalità mediche. Una precisazione necessaria, che vale a distinguere le forme tipiche di esercizio della pratica medica dal fenomeno in esame e che conduce all'interrogativo posto a fondamento della riflessione sui connotati che caratterizzano più in profondità le pratiche di potenziamento umano: perché una persona non affetta da paralisi motorie o carenze funzionali dovrebbe sottoporsi all'innesto di un impianto neuronale? O perché, ad esempio, una persona priva di particolari neurodivergenze dovrebbe assumere quotidianamente un farmaco per la cura del disturbo da deficit di attenzione?[5] Qual è, per l'appunto, l'obiettivo?

Gli obiettivi che individua il Consiglio d'Europa sono essenzialmente tre: "performance"; "looks"; "well-being"[6].

Quello più ampio e insieme più problematico è il "well-being": il perseguimento del benessere ad opera di un individuo definito "healty" entra infatti in conflitto col concetto di salute così come è stato declinato già dal 1948 dall'Organizzazione Mondiale della Sanità, che la configura non solo in senso stretto, come assenza di malattie, ma in senso lato, come "stato di *completo benessere* fisico, mentale e sociale"[7]; ed è dunque anche alla luce di questo dato che la formula "healty individual" prima richiamata va circoscritta, configurandosi in senso stretto come assenza di malattie (e, in questo caso, specificamente di quella malattia che di norma viene curata con la tecnologia medica impiegata per il potenziamento)[8]. Tale impostazione, peraltro, trova conferma anche nel nostro Codice di deontologia medica che parla, con riferimento alla medicina potenziativa, specificamente di "prestazioni non terapeutiche"[9].

4. Si allude naturalmente agli esperimenti condotti da *Neuralink*, su cui cfr. da ultimo, Kumar–Waisberg–Ong–Lee 2025, p. 521 ss.
5. In particolare, sul consumo continuativo *offlabel* del metilfenidato, un'anfetamina di norma impiegata per il trattamento dell'ADHD v., per tutti, Comitato Nazionale per la Bioetica 2013, p. 10 e nota 14.
6. La distinzione, naturalmente, riveste un valore meramente analitico, sia perché le tre finalità sono tra loro strettamente connesse, sia perché sovente esse vengono perseguite contestualmente.
7. Cfr. il primo dei principi della Costituzione dell'OMS, che recita "health is a state of complete physical, mental and social well-being and not merely the absence of disease or infermity", connotando la nozione di salute in senso bio-psico-sociale; nozione peraltro ripresa dal d.lgs. 81 del 2008, art. 2, lett. o), che la definisce come "stato di completo benessere fisico, mentale e sociale, non consistente solo in un'assenza di malattia o d'infermità" (in argomento, si v., con specifico riferimento al rapporto tra salute e potenziamento umano, Pascucci 2024, p. 146 ss.). Tra l'altro, proprio in virtù della nozione "allargata" di salute fornita dall'OMS, il *discrimen* tra intervento "curativo" e "migliorativo", tra terapia e potenziamento, appare oggi "particolarmente incerto"; con la conseguenza che sarebbe "contraddittorio permettere, da un lato, operazioni estetiche altamente invasive e sfornite di giustificazione terapeutica e negare, dall'altro, la praticabilità di potenziamenti non curativi, per quanto supportati da un valido consenso" (così Samorè 2023, p. 198). Sul rapporto fra medicina estetica e potenziativa v. anche *infra*, nota 10; anche sul rapporto fra potenziamento e cura si tornerà *infra*, nota 12.
8. L'intervento di *enhancement*, infatti, non è mai una semplice *restitutio ad integrum*: è sempre un potenziamento "oltre la salute" e "oltre la normalità". Tuttavia, va ribadito – in base a quanto prima osservato – che, se la salute è lo stato di pieno benessere fisico-psichico e sociale, allora i contorni tra malattia e normalità tendono a scolorarsi, giacché "è patologico e anormale ciò che il soggetto avverte come tale". Si offusca conseguentemente anche il distinguo tra terapia – non più intesa come mera *restitutio ad integrum* – e trattamento di potenziamento, dal momento che quest'ultimo può diventare equivalente alla terapia se "l'uso ridotto di una capacità" è "percepito soggettivamente, socialmente e culturalmente come una fonte di malessere" (così Palazzani 2015, p. 15).
9. Così recita l'art. 76 (*Medicina potenziativa*) del *Codice di deontologia medica*, approvato a Torino il 18 maggio 2014: "Il medico, sia in attività di ricerca, sia quando gli siano richieste prestazioni *non terapeutiche* ma finalizzate

Un profilo problematico emerge anche rispetto alla finalità del miglioramento del "look", dell'aspetto esteriore: la medicina estetica, infatti, viene solitamente accostata alla medicina potenziativa, perché ne condivide in larga parte le finalità (si rivolge a soggetti privi di patologie specifiche correlate all'intervento; e che, di norma, intendono migliorare il proprio aspetto esteriore secondo i propri canoni anche per incrementare il proprio benessere, a conferma della correlazione tra le diverse finalità che animano gli interventi in esame); ma la si tiene distinta, perché – come vedremo – la medicina potenziativa guarda, più che alla forma, alla *funzione*. Questo avviene anche nel nostro ordinamento: il Codice di deontologia medica inserisce infatti la medicina estetica e potenziativa nello stesso Titolo, ma vi dedica due articoli diversi[10].

Ma la finalità che più interessa in questa sede è la prima: "to improve the performance"; è infatti soprattutto rispetto a questo obiettivo che emerge il tema dianzi evocato della funzione, del miglior funzionamento, finalizzato ad incrementare le prestazioni.

In proposito vale richiamare una definizione di *human enhancement* molto più sintetica, elaborata dal Comitato nazionale per la bioetica, che coglie proprio questo aspetto, identificando tale fenomeno come "uso intenzionale delle conoscenze e tecnologie biomediche per interventi sul corpo umano al fine di modificarne, in senso migliorativo e/o potenziante, il *normale funzionamento*"[11].

E proprio il richiamo al funzionamento consente di inquadrare meglio anche il termine "normal", per evitare di sovrapporlo integralmente al concetto di "healty": si è normali se le proprie funzioni e le proprie capacità sono nella norma (o nella media); l'*enhancement* consiste dunque essenzialmente in un potenziamento funzionale, un accrescimento delle proprie capacità al di là della norma[12].

Ma torniamo alla "performance": questo elemento non solo riflette una delle ossessioni del

al potenziamento delle fisiologiche capacità fisiche e cognitive dell'individuo, opera nel rispetto e a salvaguardia della *dignità* dello stesso in ogni suo riflesso individuale e sociale, dell'identità e dell'integrità della persona e delle sue peculiarità genetiche nonché dei principi di proporzionalità e di precauzione. Il medico acquisisce il consenso informato in forma scritta avendo cura di verificare, in particolare, la comprensione dei rischi del trattamento. Il medico ha il dovere di rifiutare eventuali richieste ritenute sproporzionate e di alto rischio anche a causa della invasività e potenziale irreversibilità del trattamento a fronte di benefici non terapeutici ma potenziativi" (corsivi aggiunti).

10. Si tratta del Titolo XVI del Codice, titolato *Medicina potenziativa ed estetica*, contenente il citato art. 76, dedicato alla medicina potenziativa e l'art. 76-*bis*, dedicato alla medicina estetica.
11. Cfr. Comitato Nazionale per la Bioetica 2013, p. 5, corsivi aggiunti.
12. L'accostamento tra "*healty*" e "*normal*" *individuals*, peraltro, invita a riflettere sul complesso rapporto tra salute e normalità: in proposito, infatti, va ricordato che il campo di azione della medicina si è ampliato progressivamente, attraverso una crescente "medicalizzazione", invadendo e in certo modo erodendo il campo della normalità, fino a giungere alla "medicalizzazione del potenziabile" (cfr. sul tema Conrad 2007). In particolare, la curvatura soggettiva del concetto di salute derivante dal rilievo assegnato al benessere si fonde con le tendenze alla medicalizzazione nel concorrere a sfumare i confini tra normalità e salute: "il parametro di 'normalità' su cui misurare il mutamento – infatti – si prospetta come arbitrario e contestabile, se non addirittura con un significato potenzialmente discriminatorio verso taluni soggetti; l'antitesi salute/malattia è sempre più incerta e con zone di intersezione ai margini; specularmente, anche la distinzione tra terapia e potenziamento è contesa. Per un verso, si tende infatti a dilatare la salute in linea con la definizione accreditata dall'Organizzazione mondiale della Sanità, assecondandone la coincidenza con la percezione soggettiva del proprio stato di benessere; per un altro verso, si assiste alla medicalizzazione di molte condizioni non propriamente patologiche, come conferma l'accettazione ormai pressoché pacifica di pratiche come la chirurgia estetica o di interventi medici invasivi quali la sterilizzazione volontaria. Si aggiunga che le traiettorie di sviluppo di presidi terapeutici possono ispirare innovazioni prive di questa valenza, e viceversa, in una contaminazione reciproca senza chiari segni di discontinuità. Ciò porta complessivamente a sfumare i contorni distintivi di fisiologia e patologia e, al contempo, indebolisce la tenuta del dualismo terapia v. miglioramento e il suo impiego con valenza normativa, oltre che descrittiva" (così Palmerini 2024, p. 163).

nostro tempo – la prestazione, il risultato, la competizione[13] – ma consente anche di distinguere le forme di potenziamento che rientrano propriamente nello *human enhancement* da tutte quelle forme di "rafforzamento" delle capacità umane che caratterizzano, anche in questo caso, da sempre, la storia dell'umanità, che è anche una storia di progressivo potenziamento delle nostre capacità; lo sviluppo della tecnica, che ci caratterizza da sempre, è essenzialmente (anche) questo[14]. E permette di replicare ad un'obiezione che riaffiora sistematicamente nel dibattito sul tema: perché non vanno considerati interventi di *enhancement*, per citare un esempio tra i tanti, un paio di occhiali, cioè un manufatto tecnologico utilizzato in ambito oculistico per *potenziare* la nostra funzione visiva. Certo, si può rispondere puntualmente, osservando che l'occhiale è una tecnologia medica utilizzata per finalità mediche e, peraltro, di norma non potenzia la funzione visiva oltre la normalità (come può essere ad esempio l'innesto della c.d. "ultravista", che invece potenzia una vista "normale"). Ma manca anche qualcos'altro: manca, in particolare, quella "logica" che caratterizza lo *human enhancement*, che, come è stato efficacemente sostenuto, si fonda su "una logica globale esclusivamente prestazionale"[15], di natura performativa[16].

Quest'ultimo profilo, peraltro, assume un particolare rilievo in rapporto alla riflessione in argomento anche perché è questa la finalità fondamentale che spinge all'utilizzo delle *human enhancement technologies* in ambito lavorativo: il lavoratore "aumentato" di norma diventa tale per incrementare la propria prestazione lavorativa[17]. Un fenomeno, ad esempio, che si va rapidamente diffondendo è quello dell'impiego *offlabel* di farmaci nootropici (che integrano il c.d *enhancement* farmacologico o cognitivo) da parte di manager, piloti, musicisti, o da parte degli stessi chirurghi[18].

In realtà il potenziamento in ambito lavorativo potrebbe apportare anche vantaggi notevoli, consentendo di ridurre lo sforzo muscolare, a beneficio dei soggetti più vulnerabili o più deboli sul piano fisico; o di aumentare gli standard di sicurezza sul luogo di lavoro, riducendo la probabilità di incidenti[19]. Notevoli e numerosi sono, tuttavia, anche i rischi: che sono legati, ad esempio, all'evenienza che il potenziamento del lavoratore venga imposto o comunque "indotto" dal datore di lavoro, in violazione della sua libertà; o, per contro, all'evenienza che il potenziamento sia volontario ma "occulto", cioè tenuto nascosto – come accade spesso con l'*enhancement farmacologico* – per ottenere un indebito vantaggio nei confronti dei colleghi di lavoro[20].

Occorre dunque identificare con precisione i confini entro i quali queste pratiche possono essere consentite, segnatamente in ambito lavorativo; e la

13. Una concezione che si inquadra in una più generale visione performativa e competitiva delle relazioni umane: da questo punto di vista, le pratiche di *human enhancement* riflettono un atteggiamento che è stato efficacemente qualificato come "'accanimento' migliorativo ad ogni costo" (così Palazzani 2013, p. 211) allo scopo di assicurare il massimo rendimento.
14. In argomento si v., per tutti, Amato 2014, p. 72.
15. Così Domenella 2023, p. 5.
16. In questa prospettiva, il corpo diventa uno strumento in grado di garantire prestazioni: "secondo le logiche dello *human enhancement*" – infatti – "il valore e il senso dell'esperienza umana – e del corpo in sé – sono riconducili al numero delle *performance* con le quali poter aumentare la nostra competitività" (così Osti 2018, p. 186). In argomento si v. anche le considerazioni sviluppate *infra*, nota 31.
17. Ovviamente anche il lavoratore verrà indotto dal mercato a potenziarsi per rimanere competitivo (cfr. sul tema Palmerini 2024, p. 169). In proposito si considerino anche, ad esempio, le future applicazioni della realtà virtuale riguardanti il c.d. metaverso – annoverabile nell'ambito del *cognitive enhancement* – che vanno nella direzione della c.d. *gamification* dell'attività lavorativa, destinata a caratterizzarsi sempre più per la presenza di premi e ricompense che ne accentuerebbero notevolmente il carattere performativo e competitivo (cfr. sul tema Maio 2022, p. 49).
18. Cfr. Maio 2020, p. 522.
19. *Ivi*, p. 517.
20. *Ivi*, pp. 523-532.

loro definizione – in una prospettiva costituzionalistica – non può che partire dai limiti alla libertà d'impresa (e dunque anche, in senso lato, al datore di lavoro) espressamente previsti dal secondo comma dell'art. 41 della Costituzione, che impone all'attività economica privata il divieto di svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla salute, all'ambiente, alla sicurezza, alla libertà, alla dignità umana.

In particolare, si intendono di seguito illustrare i limiti che rientrano in senso ampio nell'ambito della *dignità*; e dunque si accennerà sia al possibile danno che il ricorso alle tecnologie di potenziamento da parte del lavoratore può arrecare alla sua dignità *tout court* ("umana" in senso lato), sia alla lesione della sua dignità "sociale", in base ad una lettura coordinata dell'art. 41, comma 2, con l'art. 3, comma 1, della Costituzione.

2. La dignità umana del lavoratore aumentato: gli interventi permanenti sul corpo del lavoratore tra alterazione morfologica e reificazione

Una delle immagini più ricorrenti, nella letteratura dedicata al lavoratore aumentato, è quella dell'esoscheletro robotico[21]. L'esempio, tuttavia, alla luce di quanto osservato in premessa, risulta improprio: lo strumento evocato, infatti, è certamente un prodotto avanzato della tecnologia robotica, ma non della tecnologia biomedica e tantomeno il suo impiego presuppone un intervento medico. Esso appare tuttavia significativo perché permette di svelare come la definizione di *human enhancement* proposta in esordio alla riflessione contenga in realtà un grande "sottinteso", che rappresenta peraltro la ragione più profonda della centralità della tecnologia medica; tecnologia che è essenziale in quanto l'intervento di potenziamento delle capacità oltre la normalità – affinché possa configurarsi propriamente come *enhancement* – deve rivestire un carattere tendenzialmente *permanente*[22].

Le funzioni potenziate, infatti, affinché possa parlarsi di un effettivo *enhancement*, debbono essere acquisite in via definitiva, non temporanea. I potenziamenti temporanei sono sempre stati possibili: è sufficiente utilizzare un microscopio o un telescopio per potenziare temporaneamente la nostra vista, o imbracciare un martello pneumatico per potenziare temporaneamente la nostra forza fisica. Il potenziamento umano, in senso proprio, corrisponde invece all'*acquisizione permanente di capacità oltre la norma*.

Acquisizione – si noti – che può realizzarsi esclusivamente a seguito di un intervento sul *corpo*: o attraverso la pratica chirurgica (ad esempio impiantando degli strumenti all'interno dell'organismo) o attraverso la farmacologia, modificando in modo tendenzialmente permanente le funzioni cerebrali mediante l'assunzione costante e prolungata di farmaci[23]. E non vale l'obiezione – sarà utile precisarlo – per cui, se si parla del lavoratore aumentato, è sufficiente che lo strumento potenziante venga utilizzato solo *finché* la persona lavora, perché, in tal caso, anche l'operaio che usa un martello pneumatico sarebbe un lavoratore in certo senso "aumentato". Il lavoratore aumentato, in questa prospettiva, è una persona che ha acquisito in modo tendenzialmente permanente delle nuove capacità e le usa in prevalenza per lavorare. L'immagine più appropriata appare dunque quella della protesi robotica *innestata*, che modifica il corpo permanentemente.

L'idea di un lavoratore al quale venga innestato – al solo scopo di migliorare la sua *performance* – un arto robotico solleva naturalmente molte perplessità sotto il profilo del rispetto della dignità umana;

21. Si v., ad esempio, Maio 2020, pp. 516-517, Maio 2024, p. 103 e Samorè 2023, p. 185.
22. Il carattere permanente dell'intervento si intreccia strettamente con il fondamentale problema della *irreversibilità* del trattamento (sia fisico, sia anche cognitivo) e della connessa tutela dell'integrità fisica del lavoratore, che emerge in relazione al divieto posto dall'art. 5 c.c. agli atti di disposizione del corpo umano quando cagionino una diminuzione permanente dell'integrità fisica del disponente (cfr. sul punto Maio 2020, p. 524). In proposito vale ricordare come di tali rischi si mostri consapevole il Codice di deontologia medica, stabilendo, all'art. 76 prima richiamato, che medico ha il dovere di rifiutare eventuali richieste ritenute sproporzionate e di alto rischio anche a causa della invasività e potenziale *irreversibilità* del trattamento a fronte di benefici non terapeutici ma potenziativi. Sul carattere irreversibile delle biotecnologie, v. Palmerini 2024, p. 166 e Meola 2017, p. 275.
23. Non va inoltre dimenticato il versante, per molti aspetti ancora inesplorato, degli interventi sul corredo genetico, su cui ci si limita, in questa sede, a rinviare, *ex multis*, a Palmerini 2024, p. 173.

e le solleva in relazione alle principali accezioni del termine che, come è noto, si presta ad essere variamente declinato. In particolare, la sua lesione potrebbe derivare, in base alla matrice kantiana, dalla riduzione dell'uomo a *mezzo*, a mero strumento[24]; o dalla violazione della sua *natura* umana[25]; o anche – in coerenza con una concezione apparentemente semplicistica, ma che in realtà coglie un aspetto essenziale – dalla alterazione della *forma* umana[26].

A tali perplessità si può tentare di rispondere con alcune affermazioni che rivestono, inevitabilmente, un carattere interlocutorio, come si addice ad una prima riflessione sul tema e atteso che su questi aspetti occorrerà riflettere a fondo nel tempo futuro. Così, volendo richiamare i tre profili di violazione della dignità dianzi evocati, merita a mio giudizio di essere indagata la plausibilità delle considerazioni seguenti: l'arto robotico detta nel dettaglio e irrimediabilmente i movimenti del lavoratore, ponendo il suo corpo al servizio della macchina; lo costringe a movenze innaturali, deumanizzandone la gestualità[27]; ne muta la fisionomia, alterando quelle "forma" umana sulla quale – come ricordato – si fonderebbe il vero riconoscimento dell'altro in quanto essere umano[28]. La lesione della dignità umana deriverebbe quindi dalla circostanza che, dall'impiego di questi strumenti, l'uomo (e anche l'uomo che lavora) risulti in certa misura sfruttato, snaturato, o deformato. Ovviamente merita di essere indagato non solo *se* ma, più verosimilmente, *in quale misura* si realizzi questo effetto.

Ma lo scenario di un operaio disposto (o perché costretto dal proprio datore di lavoro, o perché indotto dal mercato del lavoro) a sostituire il proprio braccio sano con un arto robotico innestato, fortunatamente non appare (ancora) realistico.

Esistono tuttavia delle tecnologie attualmente in uso che destano molta preoccupazione e che appaiono in grado di recare un *vulnus* alla dignità umana per certi versi ancora più profondo.

Si allude ad una particolare evoluzione dell'*Internet of things* che va sotto il nome di *Internet of*

24. Come affermato ne *La metafisica dei costumi*, "l'uomo non può essere trattato da nessuno (cioè né da un altro, e neppure da lui stesso) come un semplice mezzo, ma deve sempre essere trattato nello stesso tempo come un fine; e precisamente in ciò consiste la sua dignità (la sua personalità)" (Kant 1797/1996, pp. 333-334).

25. Muovendo dalla configurazione della dignità, propugnata dalla filosofia morale umanistica, come espressione della "vera natura" umana, per cui essa sarebbe "l'altro nome dell'umanità" (così Lipari 2006, p. 303) – sicché la sua tutela si realizzerebbe nella difesa della "vera natura" dell'uomo – l'uomo "potenziato" sarebbe un uomo "snaturato", condannato a perdere la propria dignità in quanto privato della sua umanità. In questo contesto si inseriscono anche quelle posizioni bioconservatrici la cui opposizione del potenziamento si declina nei termini di "appello alla natura", cioè come difesa di quelle caratteristiche proprie dell'essere umano che dovrebbero essere necessariamente mantenute (cfr. in proposito Stocchi 2022, p. 8).

26. Cfr. in proposito la riflessione di Margalit 2005, p. 507 ss., secondo il quale la dignità umana si manifesta nella forma umana. In questa prospettiva, la dignità risiederebbe nella facoltà, posseduta da ogni essere umano, di essere una "icona" del resto dell'umanità: il possesso della forma umana rappresenterebbe quindi il fondamentale attributo comune agli esseri umani, attraverso il quale è possibile "riconoscere" un altro essere umano come un mio simile. Tale identificazione – che si realizza attraverso l'immagine offerta dal corpo – consente di instaurare una "relazione iconica" con il resto dell'umanità.

27. Si considerino, in proposito, gli effetti prodotti dall'utilizzo delle c.d. *immersive technologies* (su cui, con specifico riferimento al loro impiego in ambito lavorativo, cfr., da ultimo, Rostova–Shirokova–Shmeleva 2023, p. 197 ss.) – ascrivibili all'ambito del *cognitive enhancement* – nell'ipotesi in cui vengano impiegate per far operare il lavoratore nel metaverso; esse, in particolare, determinerebbero un lesione della dignità del lavoratore in quanto lo porrebbero in una "condizione innaturale", derivante dall'impiego prolungato in condizione immersiva (cfr. in proposito Maio 2022, p. 57, in cui si spiegano gli effetti neurologici di tale esperienza, caratterizzata dall'attivazione dei neuroni specchio che incidono sulla configurazione neurologica reale causando anche effetti emulativi inconsapevoli; effetti che renderebbero, sotto questo profilo, l'uomo "schiavo" della macchina).

28. Cfr. *supra*, nota 26.

bodies: si tratta di dispositivi indossabili ma anche impiantabili[29], che presentano due caratteristiche: 1) interferiscono con le funzioni vitali, e in generale col funzionamento del corpo umano – e in alcuni casi sono in grado di potenziarne le capacità; 2) sono collegati alla rete Internet (e proprio questo collegamento consente il potenziamento), e in particolare raccolgono informazioni sulla persona.

La memorizzazione, va precisato, riguarda soprattutto dati biomedici: il caso più diffuso è quello dei microchip impiantabili nel corpo collegati in Rete che monitorano costantemente – e registrano – le funzioni vitali (funzionalità cardiaca, renale, ecc.). In questi casi lo scopo in realtà è medico – e dunque fuoriesce dall'ambito dello *human enhancement* inteso come utilizzo di tecnologia medica per fini non medici.

Ma in questa sede interessa specificamente il potenziamento delle funzioni; ebbene, già oggi alcuni di questi sensori impiantabili nel corpo, collegati alle Rete, possono permettere di svolgere alcune funzioni elementari, che rappresentano tuttavia, a pieno titolo, delle nuove capacità acquisite in modo permanente: aprire una porta con un gesto della mano, pagare con un movimento del braccio e più in generale controllare altri dispositivi[30]. Non è difficile immaginare che, in prospettiva, queste funzionalità aumenteranno e che si diffonderà anche il loro impiego nel posto di lavoro.

Il problema fondamentale posto da questi dispositivi è che, essendo collegati ad Internet, essi raccolgono continuamente – e, soprattutto, senza che il portatore sia in grado di interrompere il flusso – informazioni sulla sua posizione, sui suoi spostamenti, sulle attività che svolge. Ma un corpo che contiene al suo interno dispositivi che lo mantengono in costante collegamento con altri dispositivi diventa *esso stesso* un dispositivo; o, come è stato acutamente osservato, il corpo diventa un "*device* a nostra disposizione"[31].

Riguardata sotto questo profilo, la lesione della dignità si manifesta nei termini più pregnanti, che richiamano la matrice kantiana della nozione nel suo senso più profondo: una lesione intesa non solo come sfruttamento, ma propriamente come *reificazione*, come trasformazione, cioè, dell'uomo in oggetto, in cosa[32]. Non a caso l'internet dei corpi è considerata un'evoluzione dell'internet delle cose: perché, in questo contesto, la *cosa* è il *corpo*.

Tra l'altro, se queste tecnologie cominceranno ad invadere i nostri corpi e il loro valore economico continuerà ad aumentare, prima o poi qualcuno potrebbe anche ritenere che il valore delle tecnologie portate sia superiore al valore dell'uomo che le porta... E altri interrogativi sorgono spontanei: se la tecnologia innestata viene fornita dal datore di lavoro, quest'ultimo ne conserva la proprietà? E che succede se si cambia lavoro? Il dispositivo aziendale innestato resta nel corpo o viene estratto? Con quali conseguenze (fisiche, economiche, giuridiche)?

Interrogativi che aprono, evidentemente, scenari estremamente inquietanti, coi quali è verosimile che saremo costretti a confrontarci nel futuro.

29. La distinzione è tra dispositivi *body external* (braccialetti o orologi "smart", che esulano dalla nozione qui proposta di *human enhancement*), *body internal* (*pacemaker* connessi tramite *wifi*, sensori impiantabili) e dispositivi ancora più invasivi, c.d. *body melded* ("fusi" col corpo), come le interfacce neurali (sul tema, con riguardo ai fondamentali dilemmi etici e giuridici posti dalle tecnologie in parola, si v., *ex multis*, El-Khoury–Arikan 2021; in particolare, sulle interfacce neurali e le tecniche di neurostimolazione cerebrale, v. Palazzani 2015, p. 112).
30. Si tratta degli interventi di c.d. *bodyhacking*, su cui v., per tutti, Duarte 2014.
31. Così Osti 2018, p. 185. La prospettiva evocata si collega strettamente alla prima richiamata visione performativa e competitiva delle relazioni umane. Come è stato efficacemente osservato, "nella logica del potenziamento umano il corpo è strumento, macchina, è una protesi originaria che può essere modificata o anche sostituita; il tutto al fine di poter godere di prestazioni amplificate che possano farmi vincere in una logica di confronto serrato e continuativo con chi mi circonda. La corporeità è, quindi, quel congegno che, adattandolo alle mie esigenze o desideri, mi conduce in una quotidianità il cui valore è la somma delle performance che sono riuscito a fare" (così Osti 2018, p. 202).
32. Kant parla espressamente di "non reificazione" ne *La metafisica dei costumi* (Kant 1797/1996, p. 60 ss.; sulle implicazioni della nozione, configurabile anche in termini di "non mercificazione", cfr. Casillo 2020, p. 12).

3. La dignità sociale del lavoratore aumentato: il potenziamento come fonte di nuove forme di discriminazione sociale

Interrogarsi sulla dignità sociale del lavoratore aumentato impone di cambiare, per certi versi radicalmente, la dimensione dell'indagine. In questa sede rileva infatti la condizione sociale di lavoratore e il valore che viene assegnato alla posizione sociale rivestita dalla persona in quanto lavoratore, sia in termini generali, sia soprattutto all'interno della specifica comunità di lavoro nella quale opera.

Ma, soprattutto, cambia in questa sede la prospettiva (e di conseguenza il fascio di problemi che la nozione di dignità sociale impone di affrontare). Perché la prospettiva propria della dignità sociale – che deriva naturalmente dalla sua collocazione all'interno dell'art. 3 Cost. e anche, più banalmente, dal dato testuale – è quella della parità. La questione fondamentale che va affrontata in questa sede è dunque se il potenziamento incida sulla *pari* dignità sociale dei lavoratori e, segnatamente, se il lavoratore aumentato acquisisca un valore sociale superiore rispetto ai propri colleghi non aumentati, cioè goda di una maggiore considerazione sociale all'interno della propria comunità di lavoro.

A queste domande ha offerto una prima risposta, in base all'esperienza che va maturando in questi anni, la dottrina giuslavoristica, di cui varrà la pena dare conto sinteticamente.

Anzitutto, nell'ambito lavorativo, il potenziamento assicura un "vantaggio posizionale" al lavoratore rispetto ai colleghi, e nel mercato del lavoro in generale[33]. Di conseguenza, può facilmente immaginarsi che, in futuro, i lavoratori che avranno accesso (e saranno disposti) a utilizzare le tecniche di potenziamento monopolizzeranno le migliori occasioni di occupazione e di guadagno, mentre i lavoratori che non avranno accesso a tali strumenti saranno posti ai margini del mercato del lavoro, col rischio di venirne progressivamente esclusi[34].

Inoltre, può prefigurarsi una diseguaglianza, anche in termini di valore sociale, tra gli stessi lavoratori potenziati, che potrebbe fondarsi sia sulla *misura* del potenziamento, sia sulle *finalità* del potenziamento: una diversificazione, in senso lato, "censitaria", che vedrebbe le "fasce alte" (professionisti, manager, ecc.), che ricorrono al potenziamento soprattutto cognitivo per aumentare la propria *performance*, e le fasce "basse", che ricorrono al potenziamento per resistere alla fatica fisica o per sopportare lavori degradanti[35].

La compresenza di lavoratori potenziati e non potenziati – e di lavoratori "diversamente potenziati" – imporrà, infine, di affrontare in termini inediti il problema della discriminazione nel luogo di lavoro (in base al potenziamento – o ai livelli di potenziamento) e renderà necessario stabilire il divieto di trattamenti differenziati riconducibili al potenziamento (con riguardo a selezioni e assunzioni, progressioni, vicende del rapporto di lavoro e licenziamento)[36].

Sullo sfondo si staglia tuttavia una questione ben più ampia, di cui la distinzione tra lavoratori, aumentati e non, è solo un riflesso: quella del c.d. *human divide*, cioè della possibilità, che, in un futuro non molto lontano, l'umanità stessa possa suddividersi un due grandi categorie: i potenziati e non potenziati, collocati su piani differenti della scala sociale; con una netta differenziazione, dunque, che nasce sul piano delle "condizioni personali" (volendo ricondurre il fenomeno alle sue coordinate costituzionali) – modificate e rese profondamenti diseguali dal potenziamento –, suscettibile di riverberarsi anche sul piano della dignità sociale. Differenziazione, inoltre, che – verosimilmente – sarà a sua volta il riflesso delle differenti capacità economiche che consentiranno l'accesso o meno alle tecnologie di potenziamento[37].

33. Così Maio 2020, p. 536.
34. Cfr. sul tema Maio 2020, p. 534. Si consideri, ad esempio, il potenziale divario sociale generato dalle tecnologie di realtà aumentata e virtuale, in grado di tenere ai margini del mercato del lavoro i lavoratori privi di accesso a tali sistemi (cfr. sul tema Maio 2022, p. 48). Più in generale, la tendenza alla omologazione e la conseguente emarginazione di chi non si potenzia aumenterà il rischio di isolamento (economico e sociale) di chi rifiuta di potenziarsi (cfr. sul punto Comitato Nazionale per la Bioetica 2013, p. 16).
35. Così Maio 2020, p. 534.
36. Cfr. in argomento Maio 2020, p. 536.
37. Il ricorso, inevitabilmente selettivo, allo *human enhancement*, appannaggio di una ristretta *élite* economicamente avvantaggiata, appare peraltro destinato a suscitare nuovi conflitti sociali, generando "nuove condizioni

Tutte questioni, a ben vedere, molto stimolanti, ma che per il momento dobbiamo, per l'appunto, tenere sullo sfondo (auspicando, nel contempo, che la realtà non le consegni troppo presto alla ribalta).

Riferimenti bibliografici

S. Amato (2014), *La lotteria naturale è giusta?,* in L. Palazzani (a cura di), "Verso la salute perfetta. *Enhancement* fra bioetica e diritto", Edizioni Studium, 2014

R. Casillo (2020), *Diritto al lavoro e dignità*, Editoriale Scientifica, 2020

Comitato Nazionale per la Bioetica (2013), *Neuroscienze e potenziamento cognitivo farmacologico: profili bioetici*, 22 febbraio 2013

P. Conrad (2007), *The Medicalization of Society: On the Transformation of Human Conditions into Treatable Disorders*, Johns Hopkins University Press, 2007

C. Domenella (2023), *Human Enhancement e soggetto Post-Umano alla prova delle DH. Come le tecnologie digitali ci trasformano*, in "Umanistica Digitale", 2023, n. 15

B.N. Duarte (2014), *Entangled agencies: New individual practices of human-technology hybridism through body hacking*, in "NanoEthics", 2014, n. 8

M. El-Khoury, C.L. Arikan (2021), *From the internet of things toward the internet of bodies: Ethical and legal considerations*, in "Strategic change", 2021

I. Kant (1797/1996), *La metafisica dei costumi*, trad. it. e note a cura di G. Vidari, Laterza, 1996

R. Kumar, E. Waisberg, J. Ong, A.G. Lee (2025), *The potential power of Neuralink: how brain-machine interfaces can revolutionize medicine*, in "Expert review of medical devices", 2025, n. 6

M.C. Lipari (2006), *La dignità dello straniero*, in "Politica del diritto", 2006

V. Maio (2024), Smart factory*, dignità del lavoratore ed intelligenza artificiale come forma di autoapprendimento*, in S. Bellomo, O. Razzolini (a cura di), "Dignità del lavoro e civiltà digitale", Atti del Convegno svoltosi a Roma, presso l'Accademia dei Lincei, il 24 febbraio 2023, Bardi Edizioni, 2024

V. Maio (2022), *Diritto del lavoro e metaverso. Se il lavoro non è un (video)gioco*, in "Labour & Law Issues", 2022, n. 2

V. Maio (2020), *Diritto del lavoro e potenziamento umano. I dilemmi del lavoratore aumentato*, in "Giornale di diritto del lavoro e di relazioni industriali", 2020, n. 3

A. Margalit (2005), *La dignità umana fra kitsch e deificazione*, in "Ragion pratica", 2005

L. Meola (2017), *Forme di vita emergenti tra potenziamento e medicalizzazione*, in "S&F_ScienzaeFilosofia.it", 2017

G. Osti (2018), *Il corpo conteso. La questione di senso tra* human enhancement *e* achievement*,* in "Orbis Idearum", 2018, n. 1

L. Palazzani (2015), *Il potenziamento umano. Tecnoscienza, etica e diritto*, Giappichelli, 2015

di fragilità postumane" (cfr. Palmerini 2024, p. 172). Una prospettiva, questa, vagliata anche dal Comitato Nazionale per la Bioetica che, nel prendere atto della minaccia di un'inedita "società castale", prefigura il rischio di un *enhancement divide* tra *enhanced* e *unenhanced*, individuando nei secondi una categoria di soggetti "minorati" perché sprovvisti delle concrete possibilità di accedere al potenziamento (come ricorda, da ultimo, Samorè 2023, p. 205).

L. Palazzani (2013), *Potenziamento neuro-cognitivo: aspetti bioetici e biogiuridici*, in L. Palazzani, R. Zannotti (a cura di), "Il diritto nelle neuroscienze. Non 'siamo' i nostri cervelli", Giappichelli, 2013

E. Palmerini (2024), *Il potenziamento umano tra ideologia e mercato*, in "BioLaw Journal – Rivista di BioDiritto", 2024, n. 1

P. Pascucci (2024), *Dignità del lavoratore e sicurezza sul lavoro nella civiltà digitale*, in S. Bellomo, O. Razzolini (a cura di), "Dignità del lavoro e civiltà digitale", Atti del Convegno svoltosi a Roma, presso l'Accademia dei Lincei, il 24 febbraio 2023, Bardi Edizioni, 2024

Rathenau Instituut (2014), *From bio to NBIC - From medical practice to daily life*, Council of Europe, 2014

O. Rostova, S. Shirokova, A. Shmeleva (2023), *Application of Immersive Technologies to Improve the Effectiveness of Training and Staff Performance*, in O. Rostova, S. Shirokova, A. Shmeleva, "Digital Transformation: What is the Impact on Workers Today?", Springer, 2023

I. Samorè (2023), Human enhancement*, ovvero una nuova sfida per il diritto: un passo a due tra diritto costituzionale e diritti a base religiosa*, in "Stato, Chiese e pluralismo confessionale", 2023, n. 5/b

F. Stocchi (2022), *Potenziamento umano: sfide e prospettive per il futuro*, in "Humanidades e Tecnologia", 2022, n. 1

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0264 • articolo sottoposto a peer review • pubblicato in anteprima il 30 gen. 2026

Lorenzo Moroni, Nasir Muftić

Democratic governance of cybersecurity in Italy and Bosnia and Herzegovina between comparisons and perspectives

From a comparative constitutional law perspective, this article aims to investigate how democratic states, such as Italy and Bosnia and Herzegovina, should exercise their constitutional function of guaranteeing cybersecurity and, consequently, protecting fundamental rights in cyberspace through democratic governance.

Cybersecurity – Constitutional Law – Democratic governance – Fundamental rights – Technological power

La governance democratica della cybersicurezza in Italia e Bosnia-Erzegovina tra comparazioni e prospettive

Secondo una prospettiva di diritto costituzionale comparato, l'articolo intende indagare il modo in cui gli Stati democratici come l'Italia e la Bosnia-Erzegovina dovrebbero esercitare la funzione costituzionale di garanzia della sicurezza informatica e, di conseguenza, tutelare i diritti fondamentali nel cyberspazio, attraverso una governance democratica.

Sicurezza informatica – Diritto costituzionale – Governance democratica – Diritti fondamentali Potere tecnologico

L. Moroni is an Assistant Professor of Constitutional and Public Law at the University of Cagliari. N. Muftić is an Assistant Professor of Civil Law at the University of Sarajevo

This paper is a joint reflection of the two Authors. They are, however, to be attributed exclusively to Lorenzo Moroni the §§ 1, 2, 3, to Nasir Muftić the § 4, and both to Lorenzo Moroni and Nasir Muftić the § 5

1. The dominance of constitutional democracies over technological power in cyberspace

The disruptive technological progress we are witnessing, with even systems capable of self-implementation through *machine learning* mechanisms becoming established on the world stage, inevitably brings with it an exponential increase in the use of such technologies, even to cause harm to public and private entities[1].

The dangers associated with the harmful use of technology grow further if we consider that by now cyberspace and its safe accessibility by users is the necessary precondition for the full enjoyment of much of fundamental rights[2]. Reflect, for example, on freedom of speech and the rights to image, personal identity, privacy and voting.

In this regard, first and foremost, the task of promoting and protecting the full enjoyment of fundamental rights even within cyberspace rests with states. Therefore, must be rejected those ideas that by adducing the territorial encroachment of cyberspace have come to predict the eclipse of state sovereignty[3], since traditional states would be "too big, too slow, and too geographically and technically limited to regulate a global citizenry's fleeting

1. This is what emerges from the most recent studies, such as the one conducted by the Italian Association for Information Security (CLUSIT), which highlights that of the 12.732 attacks that occurred between 2020 and 2024 that can be qualified as known, serious and having a particular economic and social impact (Clusit 2025, p. 46 ff.), as many as 3.541 occurred in the year 2024 alone (*Ivi*, p. 11). This is the highest number ever. As if that were not enough, just to give an idea of the increase in the phenomenon, again in the 2020-2024 time frame, 56 percent of the total attacks recorded from 2011 to the present occurred (*Ivi*, p. 12). In other words still, it went from a monthly average of 139 incidents per month in 2019 to an average of 232 in 2023 and 295 in 2024 (*Ibidem*). To these figures, which are already sufficient in themselves to give a clear and worrying picture of today's landscape, can be added additional ones that give an idea of the impact that cyber attacks produce at the economic level. In particular, taking as reference the consequences produced by the most widespread threat, namely the *data breach*, according to the latest IBM 2024, p. 6, the global average cost of damages for a breach is $4.88 million. Whereas if one takes the cybercrime phenomenon as a whole, including direct and indirect economic consequences, then the most widely shared projections, such as that of Morgan 2023, note that the global cost will reach a total of $10.5 trillion in 2025.
2. The spread of the term *cyberspace* is due to its use by Gibson 1984. A more pragmatic definition of the term is that provided by U.S. Joint Chiefs of Staff 2011, "[A] global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers". For the connection between security and the guarantee of fundamental rights, see Giupponi 2008, p. 6 ff. On the emersion of technological power in the constitutional order and its implications, see Simoncini 2022.
3. Glenn 2013, p. 171.

interactions over mercurial medium"[4]. As argued by some, in fact, behind the "apparent weakening of the regulatory capacity of public powers due to the weakening of territorial constraints"[5], in reality would be concealed the libertarian impulses of those who would like a virtual space in which freedom can unfold unencumbered by any claim to regulation by states[6]. In fact, such a claim of "maximization of freedom"[7], appears in some way a re-proposition in virtual reality of the well-known metanarrative of "spontaneous constitutions" and its "idea of freedom as coinciding with that of liberation from the public, from the state, from political power, from the constitution, in the name of the individual and the best of all possible constitutions, the invisible one spontaneously offered to us by the market"[8].

Second, not only do states have a duty to ensure cybersecurity as a precondition for the protection and promotion of the fundamental rights of their citizens in cyberspace, but in addition, being precisely *democracies*, these states, such as Italy and Bosnia and Herzegovina, have a duty to set up cybersecurity *governance* that can be said to be democratic. Indeed, as eminently pointed out by Crisafulli, the function of Constitutions, both those more strictly of the post-World War II period such as Italy's and more recent ones such as Bosnia and Herzegovina's 1995 Constitution, is to "extend the application of the democratic principle beyond the sphere of traditional political relations, strictly understood"[9]. Therefore, while it is true that the limitation of power, as McIlwain wrote long ago, still remains "the most persistent and enduring of the essential features of true constitutionalism"[10], it is equally true that such limitation must take place according to the logic of the democratic principle. In other words, none of the forms of power, whether economic, political or, as is most relevant here, technological, can escape containment and limitation by the Constitutions[11]. And in order for this to happen even while respecting the democratic principle, there must be adequate involvement and balancing not only between public and private actors, but also between representative public institutions, think of the government and parliament.

Thus, in light of what has been said so far, the usefulness of this essay stems precisely from the comparison between two democracies such as Italy and Bosnia and Herzegovina, which are different but united by the desire to see Bosnia and Herzegovina join the European Union one day. It is certainly no coincidence that Bosnia and Herzegovina has been in official negotiations to join the European Union since March 21, 2024, but, as is well known, this is only an intermediate step that may never lead to EU membership. In fact, in order to hope to see Bosnia join the EU one day, the Balkan state must meet a whole series of requirements, not least of which is the establishment of cybersecurity governance that is not only effective but also "democratic". In this regard, comparing Bosnia and Herzegovina with Italy, which is one of the member states that has achieved the highest level of implementation of European cybersecurity legislation, this essay will seek to understand, first of all, how two democracies such as Italy and Bosnia and Herzegovina are organizing cybersecurity governance. Second, we will assess whether such governance is respectful of the democratic principle, in accordance with the requirements of their respective Constitutions (Art. 1 Italian Constitution and Art. 1 Const. Bosnia and Herzegovina), as well as Article 2 of the Treaty on European Union.

4. Boyle 1997, p. 177. On the point see also Betzu 2021, p. 168.
5. *Ibidem*.
6. *Ibidem*.
7. *Ivi*, p. 169, my translation. See, also Bauman 1998, p. 23 ff.
8. Ciarlo 2002, p. 101, my translation. Along the same lines, Irti 2000, p. 299. On the subject of state sovereignty in the face of the unprecedented challenges posed by the emergence of cyberspace, see, most recently, Barozzi Reggiani 2025, p. 1 ff.
9. Crisafulli 2015, p. 253, my translation.
10. McIlwain 1990, p. 44.
11. Luciani 1996, p. 161.

2. The governance of cybersecurity in European Union

Cybersecurity, which we can define as the defense of cyberspace infrastructure (hardware and software) and its users from external threats from any public or private entity[12], requires the provision of an adequate institutional organization to deal with the challenges and threats that daily come from the digital world. However, each state alone is unlikely to be able to concretely guarantee "security of rights" in cyberspace[13], since virtual reality, unlike material reality, is not susceptible to division into boundaries[14]. Therefore, the more the network of cooperation between states in determining a common governance of cybersecurity is extended, the more it is possible to guarantee the protection of fundamental rights in the virtual dimension[15]. This is the deeper *rationale* behind the decision of the European Union and its member states to establish a common multilevel *governance* of virtual security. Therefore, even before analyzing the characteristics of the organization of cybersecurity in Italy, it is necessary to shed light on how the European Union and broadly speaking its other member states are organizing themselves to prepare adequate *cybersecurity* governance[16].

The need to ensure the security of cyberspace infrastructure and users and to coordinate state cybersecurity regulations has led the European Union to adopt numerous acts affecting cyberspace regulation[17]. Particularly crucial among

12. This is a definition resulting from a combined reading of existing Italian and European regulations. According to Art. 2, c. 1(s) of Legislative Decree No. 138 of September 4, 2024, which refers to Decree Law No. 82 of June 14, 2021, as converted by Law August 4, 2021, No. 109, cybersecurity is to be understood as "the set of activities (...) necessary to protect networks, information systems, computer services and electronic communications from cyber threats, ensuring their availability, confidentiality and integrity and guaranteeing their resilience, including for the purpose of protecting national security and the national interest in cyberspace" (Art. 1, c. 1, lett. *a*). At the European level, however, by "cybersecurity" we must mean "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats" (Art. 2, (1), EU Regulation 2019/881). Where, "network and information system", according to Art. 4, (1) of EU Regulation 2022/2555 (NIS 2) means, according to three different but complementary meanings: a) electronic communication networks; b) one or more devices that through a program perform automatic processing of digital data; c) digital data that have been the subject of the operation of digital devices, thus those transmitted, extracted, stored, etc.
13. The expression refers to the evolution of the function of state power with respect to the protection of rights. Specifically, according to the liberal tradition, it was sufficient for the state not to act except in a repressive key to the violation of rights, whereas, with the establishment of liberal democratic constitutionalism, the state is also required to act in a preventive key to positively promote the guarantee and enjoyment of personal rights. Hence, transposing this concept to the level of security, in the words of Giupponi 2023, p. 1161, the task of the state "is not so much to guarantee a purported 'right to security' of individuals as the overall 'security of rights' of citizens" (the translation is mine). On the point, with different perspectives among them, see Baratta 2001).
14. *Contra*, in favor of self-regulation of space, see Barlow 1996; Johnson–Post 1996, p. 1371 ff. In favor, on the other hand, of agreeable state regulation of cyberspace, see Goldsmith 1998, p. 1199 ff.
15. On the importance of control and cooperation tools in achieving effective cybersecurity governance, see, above all, Pietrangelo 2024, p. 13 ff.
16. On the analysis, including diachronic analysis, of European regulation in multiple areas affecting cybersecurity, see Bederna–Rajnai 2022, p. 35 ff.
17. The European acts that, more or less directly, affect cybersecurity regulation are numerous. Limiting attention to the most relevant acts not mentioned in the core text, they range from the regulation that established the European Network and Information Security Agency (EU/2004/460), through the General Data Protection Regulation (GDPR - EU Regulation 2016/679), the Cybersecurity Act (EU/2019/881 regulation), the EU 2023/2841 regulation on the high common level of cybersecurity, and on to the Artificial Intelligent Act (2024/1689 regulation) to the Cyber Resilience Act (2024/2847 regulation) and the Cyber Solidarity Act (2025/38 regulation). For more insights into the relationship between the Artificial Intelligence Act and the Cyber Resilience Act, with particular reference to the regulation of *regulatory sandboxes*, see Bagni 2023, p. 1 ff. as well as, most recently, Bagni–Seferi 2025, p. 7 ff. and contributions cited therein. For more on the relationship between

these, however, are EU Directive 2016/1148, Network and Information System (NIS 1)[18], subsequently repealed by the more recent EU Directive 2022/2555 (NIS 2), which all member states must have implemented by October 17, 2024[19].

The current NIS 2 directive[20] fulfills the task of increasing the European Union's ability to prevent and resist cyber-attacks by strengthening EU cybersecurity and reducing threats to computer and network systems of services classified as "essential" (e.g., energy, transport, health and finance) and "important" (e.g., food, manufacturing, public administration, chemical, postal, courier, etc.)[21].

Precisely with the aim of strengthening the Union Europe's cyber infrastructure, the NIS 2 directive – following in the footsteps of the NIS 1 directive – provided for a complex system of cybersecurity governance with the pre-existing *European Union Agency for Cybersecurity* (ENISA) at its center, which is assigned the tasks of assisting and advising on the development and harmonization of member states' cybersecurity policies and regulations[22]. Alongside ENISA, the NIS 2 Directive provided for the establishment of a whole series of bodies specified in Article 1, and for what is relevant here, in para. 2, lett. a, the establishment of the national cybersecurity authorities (so-called NIS national authorities) was confirmed[23]. These NIS national authorities, assisted by *Computer Security Incident Response Teams* - CSIRTs[24], perform the crucial functions of implementing and enforcing the NIS regulatory framework, as well as overseeing its proper implementation[25]. For the successful pursuit of these goals, the NIS 2 Directive provided for the assignment of important powers to the NIS national authorities, such as "on-site inspections and off-site supervision" (Art. 32, par. 2, lett. a, NIS 2), "ad hoc audits" (lett. c), "requests to access data, documents and information" (lett. f); or powers to order those concerned "to cease conduct that infringes this Directive and desist from repeating that conduct" (Art. 32, par. 4, lett. c), "to implement the recommendations provided as a result of a security audit within a reasonable deadline" (lett. f), "to make public aspects of infringements of this Directive in a specified manner" (lett. h).

The importance of the powers held by the NIS national authorities, which in democratic states are usually the responsibility of public security authorities, combined with the crucial role they play in the successful implementation of European cybersecurity strategies suggest that the NIS direc-

the Cyber Resilience Act and other Acts concerning cybersecurity see Chiara 2022, p. 255 ff. With regard, however, to case law, with particular reference to the relationship between the protection of personal data privacy and cybersecurity see, *ex plurimis*, ECJ, judgment of October 10, 2016, C-582/14, *Breyer v. Bundesrepublik Deutschland; ECJ*, Grand Chambre, judgment of December 26, 2016, C-2013/15 and C-698/15, *Tele2 Sverige AB v. Post-och telestyrelsen*; ECJ, Grand Chambre, judgment of October 6, 2020, C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs et al.*

18. Transposed by Italy through Legislative Decree No. 65 of May 18, 2018. Both NIS 1 and NIS 2 were adopted under Article 114 TFEU, "internal market hamonization". For more insights, including critical ones, on the legal basis under Article 114 TFEU, see Poli 2021, p. 69 ff. On Article 114 TFEU, De Witte 2017, p. 59, states that "it is the most powerful tool for the expansion of the EU legislative activity".
19. Currently, 14 out of 27 states have formally transposed the NIS 2 directive. Italy has transposed NIS 2 through Legislative Decree No. 138 of September 4, 2024. For more on NIS 2, see Serini 2022, p. 241 ff.
20. For more on the system envisaged by the NIS 1 directive, see, among many others, Schmitz-Berndt–Chiara 2022, p. 289 ff.
21. Notably, NIS 2 extended the scope of NIS 1, which was limited to "operators of essential services" and "providers of digital services", see Art. 1 ff., EU Directive 2016/1148. With regard to essential and important services, see Arts. 1-3 and Annexes 1 and 2, EU Directive 2022/2555 (NIS 2).
22. See Arts. 3 ff. of EU Regulation 2019/881. With regard to the regulatory context, however, Regulation EU/2019/881 proceeded to repeal Regulation EU/526/2013, which, in turn, had proceeded to repeal Regulation EC/460/2004 (and its amendments EC/1007/2008 and 580/2011) by which ENISA was established.
23. The establishment of the NIS national authorities was already provided for in Article 8 of NIS Directive 1.
24. See Art. 1(1)(a) and Art. 10 ff., EU Directive 2022/2555 (NIS 2).
25. See Arts. 1 and 8(2), EU Directive 2022/2555 (NIS 2).

tives should be applied as uniformly as possible, at least from the point of view of the establishment of the NIS national authorities[26]. But this, in fact, has not been the case.

Actually, due to the cross-cutting nature of cybersecurity policies[27] and the wide margin of discretion that each member state usually has to implement the directives, there has been heterogeneous implementation of the NIS Directive 2 within member states[28], especially in terms of how the NIS national authorities are established[29].

A first group of states decided to entrust the role of NIS national authority to multiple independent administrative authorities or technical regulatory bodies[30]. Among them, for example, Cyprus has assigned cybersecurity functions to the independent *Digital Security Authority*[31].

A second group of states, on the other hand, has assigned the role of NIS national authority to ministries or bodies dependent on them[32]. In Denmark, for example, the functions of NIS national authority have been hinged on the *Minister for Civil Protection and Emergency Planning*[33], while in Germany, pending the transposition of NIS 2, the functions remain vested in the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*), hinged on the Federal Ministry of the Interior[34].

Finally, a third group of states has decided to assign the role of NIS national authority directly to the head of government or a government agency dependent on it[35]. Consider, for example, France and Italy, whose NIS national authorities, respectively the *Agence nationale de la sécurité des systèmes d'information* and the *Agency for National Cybersecurity*, perform their functions under the influence of the French Prime Minister[36] and the Italian Prime Minister.

Faced with the multiplicity of solutions adopted by member states, the question arises as to which of the different ways of organizing governance in cybersecurity should be considered preferable. This is a question to which it is impossible to give an unambiguous answer, since much depends on the concrete functioning of each state's form of government. However, adopting the form of state as the perspective of observation, for two reasons it can be considered that in a democracy the NIS national authorities should be hinged in constitutional bodies with political representation, thus the parliament or the government.

The first reason can be traced back to the fact that NIS national authorities – as we have already seen – exercise administrative functions, such as those of inspection, audit, requesting access to data, documents and information, which traditionally have been the responsibility of the state

26. On the ability of the harmonization of cybersecurity regulation at the European level to increase the efficiency of cyber resilience, see Schmitz-Berndt–Chiara 2022, p. 307 ff. Highlighting the fragmentation of European cybersecurity regulation Eckhardt–Kotovskaia 2023, p. 150 ff.
27. They now affect almost every aspect of daily life that has an online implication, for example: buying a product in e-commerce, requesting a document online from the public administration or searching for a word on Google.
28. This obviously applies to those 14 out of 27 states that have already formally implemented the NIS 2 directive.
29. With regard to the classification into three groups, see Lauro 2021, p. 532 ff.
30. Also included in this group of member states is Cyprus.
31. Art. 30 of the Security of Networks and Information Systems (Amendment) Law of 2025, (Law 60(I)/2025) amending The Security of Networks and Information Systems Law of 2020, (Law 89(I)/2020). Pending the formal implementation of NIS 2, Luxembourg also belongs to this set, having assigned cybersecurity functions to independent authorities such as the *Institut Luxembourgeois de Régulation and the Commission de Surveillance du Secteur Financier*, depending on their areas of responsibility, on this point, see Article 3(1) and (2), A372 Loi du 28 mai 2019.
32. Included in this group of member states are Spain; Ireland; Malta; Poland; Latvia; the Netherlands; Finland; Sweden; Slovenia; Bulgaria; Greece; Croatia; Lithuania, Estonia.
33. Chapter 3, § 20, Law No. 434, Act on measures to ensure a high level of cybersecurity (NIS 2 Act).
34. See Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 40, ausgegeben zu Bonn am 29. Juni 2017, p. 1885 ff.
35. Included in this group of member states are Belgium; Slovakia; Romania; Portugal; and Austria.
36. France still needs to transpose the NIS 2 directive.

and are exercised by public security authorities directly subordinate to government ministries, such as the Ministry of the Interior, Justice or Defense[37].

The second reason is that NIS national authorities assist member states in cybersecurity *policy-making* work. Consider, for example, the establishment of the "National cybersecurity strategy" which defines the policies and related economic resources that each state adopts on cyber security. On this point, Article 7 of the NIS 2 Directive merely provides generically that such national strategies are to be adopted by "each member state" (Art. 7, par. 1). In this way, the NIS 2 Directive would seem to open up the possibility that such cybersecurity policies can be adopted as much by the government or parliament as by administrative authorities acting independently of constitutional bodies endowed with political representation, as a NIS national authority can theoretically be. But even assuming the hypothesis that the National cybersecurity strategy can be adopted only by the government or parliament, nevertheless the NIS national authorities play a crucial role in drafting these policies. The case of Italy is emblematic, where the "National cybersecurity strategy" is adopted by the Prime Minister (after consultation with the interministerial committee for cybersecurity)[38], but is prepared by the Italian NIS national authority, called the National Cybersecurity Agency (ACN)[39].

For these reasons involving the exercise of administrative functions traditionally the responsibility of states and the involvement in cybersecurity policy work, we believe that NIS national authorities should be hinged in the government or parliament. Consequently, on the other hand, it raises concerns about assigning the functions of NIS national authorities to bodies that carry out their activities independently of constitutional bodies with political representation, such as independent administrative authorities. Indeed, it is certainly true that independent administrative authorities have contributed to the evolution of governance systems in the direction of greater efficiency, including through the reevaluation of the relationship between the public and private sectors, making it possible to solve important problems in the functioning of modern democracies[40]. However, it is equally true that independent administrative authorities, by operating unbound from the circuit of democratic legitimacy (in favor, instead, of technocratic legitimacy)[41], do not prevent the risk that they may one day acquire significant autonomy in the exercise of public power in cybersecurity matters not adequately counterbalanced by full and effective democratic oversight of parliament.

3. The governance of cybersecurity in Italy

With the implementation of the NIS 2 directive by Legislative Decree No. 138 of September 4, 2024, the NIS national authorities of the member states, including Italy[42], in addition to participating in the exercise of the policy-making function – for example, by decisively assisting policymakers in the drafting of the "National cybersecurity strategy"[43] –, they are also called upon to exercise functions of traditional state competence – such as those of supervision, implementation and especially enforcement of the NIS directives[44] –. Added to this, as repeatedly mentioned, is the fact that today cyberspace represents the main context for the exercise of many of the fundamental rights, so protecting

37. See, for example, art. 32 NIS 2 directive.

38. See, art. 4, Decree Law No. 82 of 2021.

39. See, respectively, Art. 2, c. 1(b), and Art. 7, c. 1(b), L.D. No. 82/2021.

40. See, Giraudi–Righettini 2002, p. 202 ff.

41. Donati 2017, p. 2. Also on the topic of the legitimacy of independent administrative authorities, see, among many others, Amato 1997, p. 645 ff.; Pajno 1996, p. 109; Cheli 2000, p. 130; Corletto 2003, p. 114; Riviezzo 2005, p. 338, more recently, Manetti 2023, p. 782 ff.

42. For more on the state's exclusive competence in external (art. 117, c. 2, lett. d, Const.) and internal (art. 117, c. 2, lett. h, Const.) security, as well as on the qualification of security, and consequently cybersecurity, in terms of function see Moroni 2024, p. 181 ff., as well as doctrine cited therein.

43. With regard to content, see Article 9, Legislative Decree No. 138 of 2024.

44. See Articles 10 and 34 ff., Legislative Decree No. 138 of 2024. On the role of sub-state entities in achieving cybersecurity objectives, as outlined in the DDL Cybersecurity (AC1717), see Giannelli 2024, p. 15 ff.

its security no longer means only protecting the state from internal or external aggression, but also guaranteeing its citizens the exercise of fundamental rights in virtual reality.

Because of the pervasiveness that the issue of cybersecurity has, it is necessary to have forms of parliamentary oversight of the activities of NIS national authorities and, in addition, to ensure transparency of their work. This is particularly true when these authorities are hinged in the government or, even more so, when they are independent administrative authorities.

In this regard, the Italian case is particularly interesting. The functions of NIS national authority, as well as "single NIS contact point" between the national authorities and the Commission and ENISA, are assigned by Decree Law No. 82 of 2021 first and Legislative Decree No. 138 of 2024 later to the National Cybersecurity Agency (ACN)[45]. In particular, the ACN is a government intelligence agency that performs its functions under the influence of the Prime Minister[46]. In fact, the Prime Minister has high-level direction and overall responsibility for cybersecurity policies and, in addition, has the power to appoint and dismiss the Director and Deputy Director of the Agency[47]. In addition, for the effective implementation of the NIS discipline at the sectoral level, ACN and the Prime Minister's Office are also supported by 9 ministries, which, each for matters within its competence, perform the functions of NIS sector authority[48].

However, while legislator's desire to concentrate power in cybersecurity matters in the head of the Government[49] is evident, the attempt to strengthen the parliamentary function of oversight of the executive power is equally evident. Indeed, the representative body of the electoral body, in addition to having at its disposal the classic institutions of parliamentary control of the Government[50], exercises specific control functions over the activities of the Prime Minister and the National Cybersecurity Agency. In particular, the Parliamentary Committee on the Security of the Republic (so-called COPASIR) is the body through which Parliament carries out its oversight function over the policy-making activity on cybersecurity[51]. This function, in particular, is carried out by COPASIR through multiple attributions that were not changed by the more recent Legislative Decree no. 138 of 2024, such as the power to request a hearing of the President of ACN[52] and the power to express prior opinions on the adoption of regula-

45. In this regard, see in conjunction with Articles 5 and 7 (functions) of Decree-Law No. 82 of 2021, and Articles 1(2)(e) and 10 (functions) of Legislative Decree No. 138 of 2024.
46. The ACN is endowed with some margins of independence. Pursuant to Article 5, Decree-Law No. 82 of 2021, it has regulatory, administrative, property, organizational, accounting and financial autonomy, within the limits of the decree itself.
47. Art. 2, c. 1, Decree Law No. 82 of June 14, 2021, as converted by Law No. 109 of August 4, 2021. For the sake of completeness, it is necessary to point out that a Cybersecurity Core is permanently established at ACN. This is a body that performs the function of supporting the Prime Minister's Office in aspects related to prevention, preparation of crisis situations and activation of alert procedures in the field of cybersecurity, and is composed of the Director General of the ACN, who chairs it, a military adviser to the Prime Minister's Office, a representative of the Department of Security Information (DIS), a representative of the Department of Civil Protection of the Prime Minister's Office and, for the handling of classified information, also a representative of the Central Office for Secrecy (si v. Art. 8, Decree-Law No. 82 of 2021).
48. Art. 11 of Legislative Decree No. 138 of 2024. Moreover, pursuant to Article 12 below, these NIS Sector Authorities sit on the permanent table for the implementation of the NIS framework that has been established at the NCA.
49. Caramaschi 2022, p. 76 ff. On the verticalization of cybersecurity power within the Executive, see Longo 2024, p. 328.
50. Inquiries, fact-finding investigations, hearings, questions, interpellations and motions.
51. The functions of COPASIR specifically provided for with regard to the Government's cybersecurity activity are in addition to the functions useful for the conduct of parliamentary oversight that are attributed by Law No. 124 of 2007, Art. 30 ff.
52. Art. 5, c. 6, l.d. No. 82 of 2021.

tions defining: a) the organization and functioning of ACN[53]; b) the allocation of the annual sums necessary for the functioning of ACN[54]; c) the procedures for the conclusion of public contracts of ACN[55]; d) the labor relationship with the employees of ACN[56]. In addition, again with the aim of keeping Parliament informed of ACN's activities, the Prime Minister must send both Parliament and COPASIR an annual report on ACN's activities in the previous year[57].

Thus, we cannot say that in the Italian system Parliament has no form of control of the Government in exercising the policy-making function in cybersecurity. Despite this, the system envisaged in Italy still has certain criticalities.

Indeed, given the pervasiveness of cybersecurity and the transversal nature of the matters it covers, for two main reasons the role and functioning of COPASIR appears not entirely adequate to guarantee a sufficient level of transparency of the activity of controlling political direction in cybersecurity[58].

The first reason, specific to the body itself, is due to the fact that COPASIR is designed to perform its functions with a high level of confidentiality because of its task of supervising the proper conduct of the *intelligence* activity of the Intelligence System for the Security of the Republic[59]. For example, think of its composition, which is limited to only 5 deputies and 5 senators plus the two Presidents of the Chamber of Deputies and Senate[60], or the obligation of secrecy, even after the conclusion of office, to which anyone who has acquired in the performance of his or her duties information relating to COPASIR's activities is bound[61].

The second reason, a systematic one, concerns the fact that from the establishment of the NIS authority in the Prime Minister's Office and the assignment of the Government's parliamentary oversight role primarily to COPASIR, comes an excessive concentration of power at the top of the Government. For this reason, even in the field of cybersecurity can be detected the gradual shift in balance from the legislative to the executive body that doctrine has long recorded in other areas as well[62]. Indeed, the Prime Minister plays a pivotal role not only within the Security Information System and in matters of state secrecy[63], but also within COPASIR itself. For example, COPASIR must necessarily have the consent of the President of the Council in order to obtain information and copies of acts or documents to which "confidentiality" has been opposed because of the danger they may pose to the security of the Republic[64].

53. Art. 6, c. 3, l.d. No 82 of 2021.
54. Art. 11, c. 3, l.d. No. 82 of 2021.
55. Art. 11, c. 4, l.d. No. 82 of 2021.
56. Art. 12, c. 8, l.d. No 82 of 2021.
57. Art. 14, l.d. No. 82 of 2021. On this point, see also Lauro 2021, p. 541, as well as Caramaschi 2022, p. 79 ff.
58. *Ivi*, p. 542, calls the role of COPASIR "*limiting* with respect to the breadth of areas it now presides over and *limited* both in composition and in forms of publicity".
59. *Intelligence* activity must be carried out in accordance with the Constitution, the laws and the exclusive interest and for the defense of the Republic. On the composition of the Intelligence System for the Security of the Republic see Art. 2, c. 1, of Law No. 124 of 2007.
60. Art. 30, Law No. 124 of 2007.
61. Art. 36, Law No. 124 of 2007.
62. In this regard, among many, see the contributions in Siclari 2008, as well as, recently, with particular reference to sources, Cardone 2023. Still on the subject of shifting the balance in cybersecurity governance, Lauro 2021, p. 542, notes the progressive tendency to marginalize the main seats of concerned powers (e.g., Parliament) in favor of restricted and detached seats (e.g., special parliamentary commissions).
63. In particular, if already in the previous set-up outlined by Law No. 801 of 1977 the President of the Council held a pivotal role in matters of intelligence services, such a central function was further strengthened with the reform of the organization of *intelligence* activity brought about by Law No. 124 of 2007, on this point see, on all, Giupponi 2010, p. 1 ff., as well as Giupponi 2017, p. 856 ff.
64. Art. 31, cc. 7 and 8, Law. No. 124 of 2007. Further examples from which the importance of the role of the President of the Council with respect to COPASIR can be inferred, for example, from Art. 31, c. 2, l. no. 124 of

In essence, COPASIR, because of the particular secrecy of its work and the "confidentiality" with which it routinely works in close contact with the head of the Government, does not appear to be the entirely adequate body to guarantee on its own a sufficient level of transparency even outside of Parliament[65]. Instead, the Chamber of Deputies and Senate would be more appropriate bodies to ensure transparency if they were more involved. Looking to the future then, there are many interventions that the Italian legislature could implement to involve parliamentary chambers to a greater extent[66]. Consider, for example, the provision of semiannual or four-monthly public parliamentary hearings of the ACN, or the establishment of a new *ad hoc* bicameral parliamentary committee to monitor the activities of the Government, whose greater representativeness of composition and publicity of its work would ensure adequate knowledge of the decisions taken on cybersecurity. It should not be forgotten, in fact, that "the apparatus of democracy has transparency as its rule, and secrecy is an exception"[67]. And this is all the more true for security in cyberspace, which now intersects all fields of daily life.

4. The governance of cybersecurity in Bosnia and Herzegovina

In the age of digital interdependence, cybersecurity has become not only a technical necessity but a fundamental element of state sovereignty, economic resilience, and protection of fundamental rights. This has become a truism in the 21 century Europe, which states as well as the EU have legislated and adopted policies in this matter. Bosnia and Herzegovina (BiH), however, presents an instructive case where constitutional complexity, institutional fragmentation, and weak governance have left the country exposed to mounting cybersecurity threats without a coherent or effective national response.

The Constitution of Bosnia and Herzegovina, annexed to the Dayton Peace Agreement of 1995 which ended the war, provides no explicit mention of cybersecurity. Yet the issue implicates multiple constitutional provisions. The preamble of the state Constitution proclaims that Bosniacs, Croats, and Serbs, as constituent peoples (along with Others), and citizens of Bosnia and Herzegovina are "committed to the sovereignty, territorial integrity, and political independence of Bosnia and Herzegovina in accordance with international law". The institutions on the state level[68], according to Article III(1), are responsible for matters of foreign policy, international trade, customs, defense, and general security-areas inherently tied to cybersecurity in the digital era. However, the country's constitutional arrangement is highly decentralized and labeled as "sui generis" by the state's Constitutional

2007, under which it is necessary for COPASIR to obtain the consent of the President of the Council in order to hear an employee of the Security Intelligence System, or from Art. 31, cc. 14 and 15, l. No. 124 of 2007, which stipulates that COPASIR may order access and inspections to the offices of the Security Information System only once prior notice has been given to the President of the Council, who may defer their execution in case of danger of interference with ongoing operations.

65. Moreover, there are not a few obstacles to the disclosure of secrecy in Parliament and, in addition, it is not so easy to assert the political and legal responsibility of the Government. On this point, see Bifulco 2017, p. 1115 ff.; Luciani 2013, p. 22 ff.

66. On the level of instruments of parliamentary control, Lauro 2021, p. 542, proposes the holding of annual sessions of effective control and discussion on defense and cybersecurity issues, which, therefore, go beyond "the mere acknowledgement of the Reports transmitted by the competent instances".

67. Barile 1987, p. 29; Bobbio 1991, pp. 106 and 88; Anzon 1976, p. 1761; Bifulco 2017, p. 1101.

68. The state institutions refer to the institutions at the level of the state government and not lower levels. Bosnia and Herzegovina has a complex governmental structure, It consists of the state-level government, the two entities (Federation of Bosnia and Herzegovina and Republika Srpska) and Brcko District. Moreover, the entities are asymetrical as Federation of Bosnia and Herzegovina consists of 10 cantons, while Republika Srpska fails to replicate any lower-level construction. Each of the levels of government mentioned here have their own legislature, executive and judiciary, except for cantons which judiciary is regulated mostly at the level of Federation of Bosnia and Herzegovina.

court[69]. Bosnia and Herzegovina consists of two entities – the Federation of BiH and the Republika Srpska (RS) – alongside the self-governing Brčko District. Each level of government possesses its own legislative and executive apparatus as well as the judiciary.[70] This division of powers creates legal ambiguity over which institution is competent to develop and implement cybersecurity policies. The Constitution is explicit as it suggests that the powers not explicitly assigned to the state level belong to the lower levels of government.[71] The lower levels of government may agree that the state level may assume their powers[72]. Although the matter of defense was not designated as a power of the state, the entities agreed to empower it in this matter.[73] Moreover, assignment of powers is influenced by an additional player – the Office of High Representative (OHR), an international body tasked with supervising the civilian implementation of the Dayton Peace Agreement.[74] In practice, this role is filled by a foreign diplomat or politician who holds extensive powers.[75] The most significant authority of the OHR stems from the so-called "Bonn Powers," granted in December 1997 by the Peace Implementation Council[76]. These powers enable the OHR to remove public officials who breach the obligations of the Dayton Agreement, as well as to impose laws and enact binding measures necessary to secure the enforcement of the General Framework Agreement for Peace. Since then, the OHR has had the unilateral ability to amend entity constitutions, pass legislation, and dismiss officials. The extent to which these powers have been exercised has varied over time, depending both on the individual serving as High Representative and the prevailing dynamics within the Peace Implementation Council. For example, Paddy Ashdown, one of the former High Representatives, imposed 104 laws in his first year in office between May 2002 and May 2003[77].

Bosnia and Herzegovina's political system is designed with numerous mechanisms that allow both the entities and representatives of constituent peoples to block any government decision they perceive as contrary to their interests. Rather than being citizen-centered, the system is built on a power-sharing model between the three constitu-

69. Constitutional Court of Bosnia and Herzegovina, decision number U9/ 58-III, 30. 06. i 01. 07. 2000.

70. Harun 2017, pp. 14 ff.

71. The Bosnia and Herzegovina Constitution Article III 3 stipulates: "All governmental functions and powers not expressly assigned in this Constitution to the institutions of Bosnia and Herzegovina shall be those of the Entities".

72. The Bosnia and Herzegovina Constitution Article III 5 stipulates: "Bosnia and Herzegovina shall assume responsibility for such other matters as are agreed by the Entities; are provided for in Annexes 5 through 8 to the General Framework Agreement; or are necessary to preserve the sovereignty, territorial integrity, political independence, and international personality of Bosnia and Herzegovina, in accordance with the division of responsibilities between the institutions of Bosnia and Herzegovina. Additional institutions may be established as necessary to carry out such responsibilities".

73. Harun 2017, pp. 14 ff.

74. The Dayton Peace Agreement defines the Office of High Representative. Its central part, the General Framework Agreement has eleven Annexes. Annex 10 (the Agreement on Civilian Implementation) defines the mandate of the High Representative as it follows: "the designation of a High Representative, to be appointed consistent with relevant United Nations Security Council resolutions, to facilitate the Parties' own efforts and to mobilize and, as appropriate, coordinate the activities of the organizations and agencies involved in the civilian aspects of the peace settlement by carrying out, as entrusted by a U.N. Security Council resolution, the tasks set out below". A significant development occurred in 1997, when the Peace Implementation Council (PIC) has endowed the OHR with a power to make binding decisions. The Bonn Powers grant the High Representative in Bosnia and Herzegovina broad authority to impose laws, remove elected and appointed officials, and ensure implementation of the Dayton Peace Agreement. These powers effectively allow the OHR to override domestic institutions in order to maintain peace and stability.

75. The list is available at the Office of the High Representative website.

76. *Ivi*.

77. Zvijerac 2021.

tionally recognized constituent peoples – Bosniaks, Croats, and Serbs – and the two entities[78]. Each of these groups holds guaranteed representation in legislative bodies and, in practice, is also assured positions within the executive and judicial branches. Additionally, with the exception of Republika Srpska, governments can be entirely paralyzed if the majority of representatives in the upper chamber of the legislature oppose necessary decisions[79]. This has led to prolonged institutional gridlock; for example, both the state-level government and the government of the Federation of Bosnia and Herzegovina have been effectively blocked for four years, rendering the results of past elections unenforceable. Further obstruction is possible through the executive branch, which can delay or refuse judicial appointments – such as appointments to the Constitutional Court. Compounding these structural dysfunctions, the constitutional framework itself infringes upon fundamental human rights. The European Court of Human Rights has repeatedly found that the political system discriminates against individuals who do not belong to one of the three constituent peoples, denying them the right to stand for election or to hold high public office. This was established in landmark cases of Sejdić and Finci v. Bosnia and Herzegovina[80], Zornić v. Bosnia and Herzegovina[81], Šlaku v. Bosnia and Herzegovina[82], and Pilav v. Bosnia and Herzegovina[83]. Despite these rulings, the country has failed to implement the required changes due to persistent political deadlock and the inability to reach consensus on constitutional reform.

The state-level institutions, such as the Ministry of Security of Bosnia and Herzegovina, claim constitutional competence to address issues of national security, including cyber threats[84]. Currently, there are several laws on the state level which concern cybersecurity matter, such as the laws governing electronic signature, electronic transactions, and cybercrimes and criminal procedure[85]. The state already exercises powers in this domain without a proper cybersecurity framework. Therefore, the ongoing standstill has resulted in a lack of coherent cybersecurity governance at the national level. On the other hand, the exact cybersecurity framework to be adopted should be relatively predictable. As a striving member state of the EU, Bosnia and Herzegovina entered into a Stabilisation and Association Agreement which requires it to adapt its law to the EU acquis and to establish a free-trade zone with the European Union, as well as to refrain from passing laws which are contrary to the acquis[86].

At present, BiH does not have an adopted national cybersecurity strategy. Efforts to draft such a strategy – led by the Ministry of Security with the technical support of the Organization for Security and Co-operation in Europe (OSCE) – have stalled due to political disagreement over the state-level competencies in this domain. Republika Srpska has instead developed its own cybersecurity policies, which remain separate from national efforts, thus exacerbating the legal and institutional divide[87]. It adopted the Law on Information Security in 2011. The law addressed data protection and established institutional mechanisms responsible for

78. Tahir–Muftić 2023.

79. The constitutional structure of the country can be described as consonciation as it allow ethnic groups vast veto powers. See more at Merdzanovic 2016.

80. *Sejdic and Finci v. Bosnia and Herzegovina* (27996/06 and 34836/06), European Court of Human Rights.

81. *Zornic v. Bosnia and Herzegovina* (3681/06), European Court of Human Rights.

82. *Slaku v. Bosnia and Herzegovina* (56666/12), European Court of Human Rights.

83. *Pilav v. Bosnia and Herzegovina* (41939/07), European Court of Human Rights.

84. See: *Strategy for establishment of CERT* published at the website of the Ministry of Security.

85. Law on Electronic Signature of BiH, Law on Electronic Legal and Business Transactions of BiH, Law on Prevention of Money Laundering and Financing of Terrorism in BiH, Criminal Code of BiH (parts which deal with copyright abuse), then Law on Protection of Copyright Abuse Acts, then Law on Protection of Criminal Offenses of Criminal Procedure of BiH, Law on Protection of Confidential Data of BiH, and Law on Communications of BiH.

86. Stabilisation and Association Agreement.

87. See the Government of Republik of Srpska website.

the development, implementation, and oversight of information security policies. One of the outcomes of this legal framework was the creation of the Computer Emergency Response Team of the Republic of Srpska (CERT-RS), which was designated as the entity-level CERT and became fully operational in 2015[88]. Building on this foundation, the Republic of Srpska adopted the Law on the Safety of Critical Infrastructures in 2019 and subsequently introduced the Strategy for the Fight against Cybercrime for the period 2019–2023, further expanding its normative and strategic approach to cybersecurity. The absence of a functional national Computer Emergency Response Team (CERT) further exemplifies this governance paralysis. Although the state-level authorities proposed the establishment of BiH-CERT as early as 2011, political blockages have prevented its creation. Republika Srpska maintains its own CERT operating independently from any state-level coordination mechanism. The Federation of BiH lacks an equivalent body, but it attempted to pass the equivalent law on information security in this entity in 2022[89]. The attempt was unsuccessful, rending both level of Federation BiH and the state level deregulated. There is one exception on the state level – the Ministry of Defense of Bosnia and Herzegovina, which has its own policies in this matter. To sum the current state, we can cite the EU Commission's words in the Report for Bosnia and Herzegovina for 2023: "Bosnia and Herzegovina does not have a comprehensive legislative framework on the security of networks and information systems (a law on information security is in place only in the Republika Srpska entity), and made no progress in adopting a country-wide strategy. Moreover, the country made no progress in designating a country-wide single point of contact responsible for coordination and cross-border cooperation. Bosnia and Herzegovina needs to establish a network of computer security incident response teams (CSIRT) to facilitate strategic cooperation and the exchange of information; a CSIRT is operational only at the Ministry of Defence and in the Republika Srpska entity."[90]. In practice, it means that cybersecurity incidents are often handled in an ad hoc fashion by law enforcement bodies, with limited technical capability and no unified strategic oversight.

The consequences of this fragmented approach are profound. A combination of outdated systems, weak institutional capacity, and a low level of digital literacy has created fertile ground for cybercrime, disinformation, and digital espionage. The Global Cybersecurity Index ranks BiH alarmingly low, and research conducted by Euronews has highlighted that the country faces the highest exposure to cybersecurity threats in Europe. In the absence of a coherent defense, both public institutions and private citizens remain highly vulnerable to phishing attacks, ransomware, identity theft, and other forms of cyber intrusion. The lack of a comprehensive cybersecurity strategy not only leaves the country exposed to external threats but also undermines trust in digital services, e-commerce, and e-government key drivers of economic modernization.

The gridlock has seemed to be starting to get unlocked a couple of years ago. Cyberattacks on BiH institutions[91] have spurred action. In May 2023, the Council of Ministers approved changes to the Ministry of Security's internal organization, enabling the creation of a CERT. This step could have marked the beginning of a coordinated response to cyber threats, aiding both the fight against cyberattacks and alignment with EU cybersecurity standards. The Ministry of Security planned to recruit CERT staff, develop a comprehensive operational plan, and join international CERT networks to share threat intelligence and best practices[92]. However, two years forwards, there seems to be no substantial progress. In fact, to discuss the issue of democratic governance requires a willingness to govern cybersecurity on the national level first, but so far it seems that the increased exposure of BiH institutions and citizens fails to change it.

88. The CSIRT RS is also part of the CSIRT system known as "Western Balkans".

89. See the FBIH Government website from 2022 post.

90. EU Commission, *Bosnia and Herzegovina 2023 Report*, SWD(2023) 691.

91. Available at: radiosarajevo.ba website.

92. Report of the Council of Ministers for 2023.

5. From comparison to perspective: towards democratic governance of cybersecurity in Bosnia and Herzegovina

A comparison between the Italian and Bosnian legal systems in the field of cybersecurity reveals a picture of considerable systemic complexity, marked by fundamental structural differences that require Bosnia and Herzegovina (BiH) to undertake immediate reform and adaptation in order to aspire to future integration into the European Union.

Italy, in fact, although with significant margin for improvement in terms of cybersecurity governance, remains one of the very few countries in the world to have obtained the maximum score from the International Telecommunication Union's *Global Cybersecurity Index for 2024*, unlike Bosnia and Herzegovina, which, on the contrary, is the European country with the lowest score.

From the point of view of cybersecurity governance, the study shows that there is no doubt that Italy, unlike Bosnia, has benefited from its membership of the European Union for at least two reasons. The first is that the EU, having moved early to outline the essential elements of cybersecurity governance, has substantially reduced the impact of internal political instability on the process of establishing cybersecurity governance. In fact, from a technical and political point of view, it is much easier to prepare internal legislation implementing EU directives, such as NIS 1 and 2, than draft laws that provide for a complicated system of inter-state management and cooperation on cybersecurity from the beginning. This, combined with the prescriptive force of EU directives and the sanctions mechanisms for non-compliant states, has led almost all European states, including Italy, to achieve a high degree of implementation of NIS 1 and 2. The second reason why Italy, unlike Bosnia, has benefited greatly from its membership of the European Union is that cybersecurity governance is characterized by profound and essential elements of homogeneity among European states, which therefore guarantees a very high level of cooperation within the European space. Focusing solely on institutional bodies, for example, all European states are required to adhere to the complex European cybersecurity system, which is centered on European ENISA and the national NIS authorities assisted by CSIRT emergency response units. In short, this is a system that has profound elements of homogeneity, thanks to which it has been possible to create an integrated system to combat threats from the virtual world that involves all 27 member states in a synergistic manner.

Clearly, despite these positive elements, there are some areas that need to be worked on to improve the system. As already discussed, apart from some differences in the speed of transposition of the NIS 2 Directive – which, however, is not a cause for excessive concern – it would certainly have been desirable to have a more uniform implementation with regard to the attribution of the role of national NIS authority to representative bodies, such as the government or parliament, rather than to independent administrative authorities, as was the case in Cyprus, for example.

The situation in Bosnia and Herzegovina today is quite different. In stark contrast to Italy, the fact that Bosnia and Herzegovina does not belong to a supranational organization such as the European Union has meant that the numerous problems with the effectiveness of the government's organization in Bosnia have been reflected in the governance of cybersecurity. As noted above, the combination of factors attributable to extreme constitutional complexity, institutional fragmentation, and weak government effectiveness has meant that Bosnia and Herzegovina still does not have a common cybersecurity system between the Federation of Bosnia and Herzegovina and the Republika Srpska capable of dealing with the growing threats from the digital world. As a result, the burden of developing a policy to combat cybercrime falls entirely on the state level, where the Federation of Bosnia and Herzegovina has not yet managed to adopt a cybersecurity strategy due to frequent political disagreements. Political agreement, on the other hand, has been reached at the state level in Republika Srpska, since it approved a cybersecurity strategy in 2019 and has had a Computer Emergency Response Team of the Republic of Srpska (CERT-RS) since 2015. However, the usefulness of all these measures is now inevitably compromised by the fact that all the measures adopted to combat cybersecurity are limited in scope to Republika Srpska alone, leaving most of Bosnia and Herzegovina without effective protection against cyber threats. Moreover, such approach remains futile as there

is a lack of a necessary cybersecurity framework on the state level although all levels of government have interest to have a state-level framework due to their own security.

Faced with such a fragmented landscape of Bosnian cybersecurity governance, which clearly has more shadows than lights, perhaps a glimmer of hope can be found in the very fact that a cybersecurity strategy model and a CSIRT approach at least exist at the entity level in Republika Srpska and, therefore, this could serve as a starting point for BiH to then orient its entire governance towards the provisions of the European NIS 2 Directive. This is, of course, only a glimmer of hope, but it may be worth placing some hope in it, even if its feasibility seems rather remote at present, as it would require close cooperation between the actors to establish a state-level framework.

Shifting the focus from the organization of cybersecurity governance to the democratic nature of this governance, once again the comparison confirms both positive and negative aspects on both the Italian and BiH sides.

As far as Italy is concerned, it has been noted that entrusting the role of national NIS authority to the ACN is certainly a reasonable choice. This body is technically competent and is based within the Presidency of the Council of Ministers, meaning that it is subject to the control of a politically representative body. Despite these positive elements, however, it has been argued that some critical issues remain regarding the entrusting of the role of parliamentary control mainly to COPASIR, since the strict confidentiality with which it works closely with the Prime Minister, combined with the rule of secrecy that characterizes its work, risks not only excessively centralizing cybersecurity functions at the top of the government, but also failing to ensure a sufficient level of transparency outside Parliament.

As regards Bosnia and Herzegovina, it is clear that the assessment of democracy cannot be made on the basis of state governance, but only partly, on the basis of that of the entity of Republika Srpska, because it is the only one that exists and could therefore represent a first model of approximation to the governance imposed by the NIS 2 Directive. In this regard, the Republic's decision to establish the CSIRT-RS within the Ministry of Scientific and Technological Development and Higher Education, rather than, for example, within an independent administrative authority or a private company, is understandable and technically agreeable[93]. This choice resembles the one taken by Italy with regard to the ACN and, therefore, the same concerns that apply to Italy also apply to Republika Srpska, namely the danger of excessive centralization of cybersecurity governance in the executive branch and the need to ensure not only parliamentary oversight of the executive, but also adequate transparency of cybersecurity activities.

Looking to the future, while the measures to improve the structure and democratic nature of cybersecurity governance appear to be well defined, the situation is different in Bosnia and Herzegovina.

We have already seen that, in Italy, a measure that would improve both the structure and the democratic nature of cybersecurity governance would be, for example, the replacement of parliamentary control of digital security policies mainly made by COPASIR, with the provision of semi-annual or quarterly public parliamentary hearings of the ACN, or directly the establishment of a new *ad hoc* bicameral parliamentary commission to monitor the activities of the government, whose greater representativeness in terms of composition and publicity of its work would ensure adequate knowledge of the decisions taken on cybersecurity.

With regard to Bosnia and Herzegovina, on the other hand, rather than targeted interventions, it is necessary to reflect on a real path towards the establishment of cybersecurity governance, whose structure and democratic nature reflect the provisions contained in the European NIS 2 Directive, also taking inspiration from existing models such as the Italian one.

First of all, in order to bridge the gap between the structure and democratic nature of BiH cybersecurity governance and that of Italy and other EU members, it is necessary to first establish a BiH cybersecurity body, along the lines of the Italian ACN, which will be entrusted with a series of tasks, including the essential technical assistance in the adoption of a National Cybersecurity Strategy that provides for the inclusion and cooperation be-

93. Law on Republic Administration ("Official Gazette of the Republic of Srpska", No. 115/18).

tween BiH, Republika Srpska, and the Brčko District. Secondly, again in line with the provisions of Italy and the European NIS 2 Directive, the Bosnian cybersecurity body must be supported by a State-Level CERT to combat cybersecurity threats, which must also include all state and autonomous entities within Bosnia and Herzegovina. In this regard, it should be emphasized that governance at the state level cannot be achieved as long as there is a lack of consensus of Republika Srpska, Federation of BiH and the Brcko District. This is a necessary step to achieve a unified and synergistic approach. Thirdly, in order to ensure the right level of democracy and transparency in the system thus envisaged, the BiH Parliament will need to be equipped with a whole range of tools to monitor the work of the BiH cybersecurity body and the state CSIRT. In this regard, consideration should be given to setting up an ad hoc parliamentary committee for BiH digital security, accompanied by reporting obligations at set intervals. Finally, it is essential that institutional activities in the field of cybersecurity are not limited to the mere preparation and implementation of regulatory, organizational, and technological tools for the protection of digital infrastructure, but are simultaneously integrated with adequate and systematic dissemination and education of the population, which is crucial for the overall effectiveness of public policies in this area.

In conclusion, the path that Bosnia and Herzegovina must take to adapt its structure and increase the democratic nature of its cybersecurity governance is long and complex, but at the same time essential. Its success is not only a necessary condition for legitimately aspiring to join the European Union in the future, but also an essential prerequisite for consolidating effective forms of cooperation with other democratic states. In the current global context, the protection of fundamental rights can no longer be guaranteed solely within national borders: it is only through an extensive and shared cybersecurity system, transcending the territorial boundaries of Italy, Bosnia and Herzegovina, and even the European Union, that it becomes concretely possible to ensure constitutional control of technological power, as well as the effective protection and full enjoyment of fundamental constitutional rights within the digital dimension.

References

G. Amato (1997), *Autorità semi-indipendenti e autorità di garanzia*, in "Rivista trimestrale di diritto pubblico", 1997

A. Anzon (1976), *Segreto di Stato e Costituzione*, in "Giurisprudenza costituzionale", 1976

F. Bagni (2023), *The Regulatory Sandbox and the Cybersecurity Challange: from the Artificial Intelligence Act to the Cyber Resilience Act*, in "Rivista italiana di informatica e diritto", 2023, n. 2

F. Bagni, F. Seferi (2025), *Regulatory Sandboxes for AI and Cybersecurity. Questions and answers for stakeholders*, 2025

A. Baratta (2001), *Diritto alla sicurezza o sicurezza dei diritti?*, in M. Palma, S. Anastasia (eds.), "La bilancia e la misura", Franco Angeli, 2001

P. Barile (1987), *Democrazia e segreto*, in "Quaderni costituzionali", 1987, n. 1

J.P. Barlow (1996), *A Declaration of the Independence of Cyberspace*, 1996

G. Barozzi Reggiani (2025), *La* race for the cyberspace *degli Stati e il tema della cybersicurezza: tra sovranità e modelli di governance*, in "Rivista italiana di informatica e diritto", 2025, n. 2

Z. Bauman (1998), *Globalization. The Human Consequences*, Columbia University Press, 1998

Z. Bederna, Z. Rajnai (2022), *Analysis of the cybersecurity ecosystem in the European Union,* in "International Cybersecurity Law Review", 2022, n. 2

M. Betzu (2021), *Poteri pubblici e poteri private nel mondo digitale*, in "Rivista Gruppo di Pisa", 2021, n. 2

R. Bifulco (2017), *Segreto e potere politico*, in "Enciclopedia del diritto. Annali X", Giuffrè, 2017

N. Bobbio (1991), *La democrazia e il potere invisibile*, in N. Bobbio, "Il futuro della democrazia", Einaudi, 1991

J. Boyle (1997), *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, in "University of Cincinnati Law Review", vol. 66, 1997

O. Caramaschi (2022), *La cybersicurezza nazionale ai tempi della guerra (cibernetica): il ruolo degli organi parlamentari*, in "Osservatorio costituzionale", 2022, n. 4

A. Cardone (2023), *Sistema delle fonti e forma di governo. La produzione normativa della Repubblica tra modello costituzionale, trasformazioni e riforme (1948-2023)*, il Mulino, 2023

E. Cheli (2000), *Le autorità amministrative indipendenti nella forma di governo*, in "Associazione per gli studi e le ricerche parlamentari", vol. 11, Giappichelli, 2000

P.G. Chiara (2022), *The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. An introduction*, in "International Cybersecurity Law Review", 2022, n. 3

P. Ciarlo (2002), *Contro l'idea di costituzione spontanea*, in "Quaderni costituzionali", 2002, n. 1

Clusit (2025), *Rapporto 2025 sulla Cybersecurity in Italia e nel mondo*, 2025

D. Corletto (2003), *Autorità indipendenti e giudice amministrativo*, in P. Cavaleri, G. Dalle Vedove, P. Duret (a cura di), "Autorità indipendenti e Agenzie. Una ricerca giuridica interdisciplinare", Cedam, 2003

V. Crisafulli (1950/2015), *Costituzione e protezione sociale*, in "Rivista degli Infortuni e delle Malattie Professionali", 1950, n. 1, now in V. Crisafulli, "Prima e dopo la Costituzione", Editoriale Scientifica, 2015

B. De Witte (2017), *Exclusive Member States competences: is there such a thing?*, in I. Govaere, S. Garben (eds.), "The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future", Bloomsbury Publishing, 2017

F. Donati (2017), *Democrazia pluralista e potestà normativa delle autorità indipendenti*, in "Osservatorio sulle fonti", 2017, n. 3

P. Eckhardt, A. Kotovskaia (2023), *The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive*, in "International Cybersecurity Law Review", 2023, n. 4

M. Giannelli (2024), *Il contributo dei livelli di governo substatali al raggiungimento degli obiettivi del ddl Cybersicurezza*, in "Rivista italiana di informatica e diritto", 2024, n. 1

W. Gibson (1984), *Neuromancer*, Gollancz, 1984

G. Giraudi, S. Righettini (2002), *Le autorità amministrative indipendenti. Dalla democrazia della rappresentanza alla democrazia dell'efficienza*, Laterza, 2002

T. Giupponi (2023), *Sicurezza e potere*, in "Enciclopedia del diritto. I tematici, vol. V, Potere e costituzione", Giuffrè, 2023

T. Giupponi (2017), *Segreto di Stato (diritto costituzionale)*, in "Enciclopedia del diritto, Annali X", Giuffrè, 2017

T. Giupponi (2010), *Servizi di informazione e segreto di Stato nella legge n. 124/2007,* in "Forum di Quaderni costituzionali", 2010

T. Giupponi (2008), *La sicurezza e le sue "dimensioni" costituzionali*, in "Forum di Quaderni Costituzionali", 2008

H.P. Glenn (2013), *The Cosmopolitan State*, Oxford University Press, 2013

J.L. Goldsmith (1998), *Against Cyberanarchy*, in "University of Chicago Law Review", 1998, n. 4

IBM (2024), *Cost of a Data Breach Report*, 2024

N. Irti (2000), *Economia di mercato e interesse pubblico*, in "Interessi pubblici nella disciplina delle public companies, enti privatizzati e controlli", Atti del XLV Convegno di studi di scienza dell'amministrazione. Varenna, Villa Monastero, 16-18 settembre 1999, Giuffrè, 2000

I. Harun (2017), *Raspodjela nadležnosti prema Ustavu BiH* (Divison of Competences According to the Constitution of Bosnia and Herzegovina). Sveske za javno pravo | Blätter für Öffentliches Recht, 2017

D.R. Johnson, D. Post (1996), *Law and Borders: The Rise of Law in Cyberspace*, in "Stanford Law Review", 1996, n. 5

A. Lauro (2021), *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, in "Rivista Gruppo di Pisa", 2021, n. 3

E. Longo (2024), *Il diritto costituzionale e la cybersicurezza. Analisi di un volto nuovo del potere*, in "Rassegna parlamentare", 2024, n. 2

M. Luciani (2013), *Il segreto di Stato nell'ordinamento nazionale*, in "Gnosis. Rivista italiana di intelligence", 2013, n. 2

M. Luciani (1996), *L'antisovrano e la crisi delle costituzioni*, in "Rivista di diritto costituzionale", 1996, n. 1

M. Manetti (2023), *Poteri e garanzie (Autorità indipendenti)*, in "Enciclopedia del diritto. I tematici, vol. V, Potere e costituzione", Giuffrè, 2023

C.H. McIlwain (1990), *Constitutionalism: Ancient and Modern*, New York, 1947, transl. it. *Costituzionalismo antico e moderno*, il Mulino, 1990

A. Merdzanovic (2016), *'Imposed consociationalism': external intervention and power sharing in Bosnia and Herzegovina*, Peacebuilding, 2016

S. Morgan (2023), *Cybercrime To Cost The World $9.5 Trillion Annually in 2024*, in "Cybercrime magazine", 2023

L. Moroni (2024), *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, in "federalismi.it", 2024, n. 14

A. Pajno (1996), *L'esercizio di attività in forme contenziose*, in S. Cassese, C. Franchini (eds.), "I garanti delle regole", il Mulino, 1996

M. Pietrangelo (2024), *La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo*, in "Rivista italiana di informatica e diritto", 2024, n. 2

S. Poli (2021), *Il rafforzamento della sovranità tecnologica europea e il problema delle basi giuridiche*, in "AISDUE", 2021, n. 5

L. Risicato (2019), *Diritto alla sicurezza e sicurezza dei diritti: un ossimoro invincibile?*, Giappichelli, 2019

A. Riviezzo (2005), *Autorità amministrative indipendenti e ordinamento costituzionale*, in "Quaderni costituzionali", 2005, n. 2

S. Schmitz-Berndt, P.G. Chiara (2022), *One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS 2 directive*, in "International Cybersecurity Law Review", 2022, n. 3

F. Serini (2022), *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in "federalismi.it", 2022, n. 12

M. Siclari (2008), *I mutamenti della forma di governo. Tra modificazioni tacite e progetti di riforma*, Aracne, 2008

A. Simoncini (2022), *La dimensione costituzionale dell'intelligenza artificiale*, in G. Cerrina Feroni, C. Fontana, E.C. Raffiotta (a cura di), "AI Anthology. Profili giuridici, economici e sociali dell'intelligenza artificiale", il Mulino, 2022

H. Tahir, N. Muftić (2023), *Regulation of Audiovisual Media in Bosnia and Herzegovina – an Overview: Is the Cure Worse Than the Disease?*, in G. Gergely, E. Lazar (eds.), "Media Regulation During the COVID-19 Pandemic: A Study from Central and Eastern Europe", Ethics International Press, 2023

U.S. Joint Chiefs of Staff (2011), *Cyberspace, in Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, Washington DC, 2011

P. Zvijerac (2021), *Sve odluke Valentina Inzka*, Radio Slobodna Evropa, 20 July 2021

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0253 • articolo sottoposto a peer review • pubblicato in anteprima il 10 dic. 2025

Pier Giorgio Chiara, Geordie Morciano
Alessandro Vannini, Raffaella Brighi, Marco Prandini

Un approccio pratico di '*legal design*': la Guida al regolamento UE Cyber Resilience Act. Metodo, obiettivi ed impatti

Questo articolo illustra il lavoro multidisciplinare alla base della '*Guida al regolamento UE Cyber Resilience Act: un approccio di legal design*', soprattutto, dando rilevanza al metodo, nonché agli obiettivi e agli impatti attesi. La Guida intende chiarire l'applicazione del Regolamento UE 2024/2847 (Cyber Resilience Act, CRA). Al fine di ridurre l'alta complessità tecnico-giuridica del CRA, la guida adotta un approccio innovativo che combina i principi del *legal design* con competenze tecniche, informatiche e giuridiche, in materia di cybersicurezza. Le disposizioni e i meccanismi complessi del CRA sono tradotti in processi più accessibili a coloro che dovranno applicarli, riducendo pertanto il rischio di errate interpretazioni nelle fasi di pianificazione della conformità e di attuazione.

Legal design – Cybersicurezza – Cyber Resilience Act – Diritto Ue – Ricerca multidisciplinare

A practical legal design approach: the Guide to the EU Regulation Cyber Resilience Act. Methodology, goals and impacts

This article outlines the multidisciplinary work behind the '*Guide to the EU Cyber Resilience Act: a legal-design approach*' project, with a particular emphasis on its methodology, objectives, and expected impacts. The Guide aims to clarify the application of EU Regulation 2024/2847 (Cyber Resilience Act, CRA). To lower the high technical-legal complexity of the CRA, the Guide employs an innovative approach that integrates legal design principles with technical expertise, encompassing both IT and legal aspects, in the cybersecurity field. The CRA's complex provisions and mechanisms are translated into processes that are more accessible to those required to implement them, thereby reducing the risk of misinterpretation during compliance planning and implementation phases.

Legal design – Cybersecurity – Cyber Resilience Act – EU law – Multidisciplinary research

P.G. Chiara e R. Brighi afferiscono al Dipartimento di Scienze Giuridiche, mentre A. Vannini e M. Prandini afferiscono al Dipartimento di Informatica - Scienza e Ingegneria dell'Università di Bologna. G. Morciano è legal innovation specialist

A P.G. Chiara sono da attribuirsi le sezioni 1 e 3. La sezione 2 è da attribuirsi congiuntamente a P.G. Chiara, G. Morciano e A. Vannini

Questo contributo è stato sostenuto dal Progetto SERICS (PE00000014), finanziato dall'Unione Europea - NextGenerationEU attraverso il MUR nell'ambito del PNRR – Missione 4 Componente 2, Investimento 1.3

1. Introduzione

Il presente lavoro illustra gli obiettivi, la metodologia e la struttura della Guida dedicata al Regolamento (UE) 2024/2847, che introduce requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali (Cyber Resilience Act, CRA)[1]. L'iniziativa nasce con l'intento di chiarire il funzionamento del Regolamento e di tradurre requisiti normativi e tecnici complessi in misure organizzative e operative concrete, fornendo quindi indicazioni chiare e attuabili ai soggetti coinvolti nella sua applicazione, tra cui operatori economici (fabbricanti, importatori, distributori, rappresentanti autorizzati e gestori di software open source), consulenti legali ed esperti tecnici di cybersicurezza. In questa prospettiva, la Guida si configura non solo come un riferimento giuridico, ma come uno strumento pratico per la pianificazione della conformità, il coordinamento tra i diversi attori coinvolti dalle attività di compliance (internamente ed esternamente ad un'azienda) e la riduzione del rischio di errore interpretativo durante la fase di implementazione.

La Guida si distingue per l'adozione di un approccio metodologico innovativo, fondato sull'integrazione di principi di legal design e competenze tecniche, vale a dire, giuridiche e informatiche, di cybersicurezza. Il legal design contiene nel suo spettro competenze trasversali di matrice giuridica, linguistica e di design, le cui tecniche, sinergicamente applicate, permettono di rimodellare testualmente e graficamente il precetto normativo, lasciandone invariata la corretta connotazione giuridica[2]. Il punto focale di tale disciplina, e delle tecniche ad essa sottese, corrisponde ai bisogni e alle esigenze pratiche degli utenti finali specificamente identificati per il progetto di specie. Tale architettura progettuale consente, così, di semplificare e rendere fruibili contenuti normativi complessi. In particolare, colmare la lacuna epistemica tra i "classici" utenti del diritto (avvocati, giudici e autorità) e tutti gli altri utenti (cittadini, consumatori, imprese)[3].

La Guida è frutto di una collaborazione multidisciplinare tra l'area giuridica, con esperienza in diritto europeo della cybersicurezza, l'area ingegneristica, con specifiche competenze in *Operational Technology* (OT) *security*, ed infine uno specialista in tecniche di legal design. In tale contesto, è stato adottato il design thinking quale metodo operativo di riferimento, calibrandone le fasi canoniche (dall'analisi dei bisogni all'ideazione, prototipazione e validazione) agli obiettivi e alle tempistiche del progetto[4]. Tale impostazione metodologica ha consentito di realizzare un processo autenticamente multidisciplinare, nel quale

1. Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza). Per un'analisi critica del regolamento, si permetta il rinvio a Chiara 2025.
2. Hagan 2020; Koulu–Pohle 2024; Rossi–Ducato–Haapio–Passera 2019.
3. Legal Design Alliance 2018.
4. Ducato–trowel 2021.

la dimensione giuridica, tecnica e comunicativa si integrano in modo coerente e complementare.

Oltre al suo valore operativo, la Guida svolge un ruolo di ponte concettuale tra domini tradizionalmente separati (giuridico, tecnico e gestionale), promuovendo una visione integrata della cybersicurezza e della resilienza, e una cultura comune della conformità tra i molteplici attori coinvolti.

Conformandosi a questi principi, la Guida mira ad essere tuttavia strumento utile per i diretti utilizzatori del Regolamento, nel caso di specie di stampo prevalentemente tecnico, e in questo senso, dunque, anche per gli utenti "classici" del diritto, in virtù della specificità del CRA data non solo dalla complessa commistione tra l'elemento tecnico e giuridico, ma anche dall'ibridizzazione di diversi approcci regolatori (sezione 2). L'accesso ad un testo giuridico in modo chiaro è una componente essenziale di una compliance e governance efficace della cybersicurezza. Non è un caso che per rispondere alle esigenze dei professionisti a sostegno dell'attuazione del CRA, l'articolo 10 del regolamento richieda agli Stati membri di promuovere misure e strategie volte a sviluppare competenze di cybersicurezza anche attraverso la creazione di strumenti organizzativi e tecnologici. Guardando invece all'esperienza in settori più maturi, importanti esperimenti di legal design sono stati condotti in un ambito "vicino" alla cybersicurezza[5], vale a dire la protezione dei dati personali, segnatamente nell'applicazione del GDPR[6], ed in particolare dell'articolo 12.

Per garantire al contempo rigore giuridico e accuratezza tecnica, l'analisi del regolamento è stata arricchita da contributi tecnici in materia di cybersicurezza, rendendo il documento accessibile a un pubblico interdisciplinare. Il risultato è un'interpretazione operativa che mira a ridurre l'alta complessità tecnico-giuridica del Cyber Resilience Act, utile a orientare la progettazione e l'adeguamento dei processi aziendali in diversi contesti reali.

Come anticipato, il presente contributo illustra la metodologia innovativa adottata per l'elaborazione della Guida, la cui originalità risiede non soltanto nell'aver utilizzato il *design thinking*[7] quale struttura portante dell'intero processo operativo, ma anche nell'impiego mirato di tecniche di design capaci di "scomporre" la complessità del Regolamento e di "ricomporla" in un ordine concettuale chiaro, coerente e logicamente fruibile. Muovendo dalle cinque fasi del *design thinking*, le sezioni che seguono ne ripercorrono l'applicazione al progetto, illustrando per ciascuna fase le strategie e gli strumenti adottati e mettendo in evidenza il loro contributo alla costruzione di un modello interpretativo e operativo del Cyber Resilience Act.

In questa introduzione si riportano sinteticamente le cinque fasi che hanno scandito il processo. La prima fase, "Ricerca" (sezione 2.1), ha avuto l'obiettivo di comprendere i bisogni e le esigenze degli utilizzatori finali della Guida, al fine di raccogliere *insight* qualitativi e quantitativi utili all'impostazione del progetto. In linea con un approccio di co-design collaborativo, è stata definita una strategia di ricerca basata su interviste strutturate, strumenti che hanno consentito di delineare in modo realistico le aspettative, le criticità operative e le competenze degli utenti potenziali. Sulla base dei dati raccolti, infatti, il team ha delineato i profili rappresentativi dei potenziali destinatari che, nelle diverse tipologie professionali, si troveranno a utilizzare la Guida nella pratica quotidiana. La seconda fase, "Definizione & Ideazione" (sezione 2.2), è stata concepita come un unico step da un punto di vista metodologico, e ha tradotto gli insight emersi nella fase "Ricerca" in soluzioni progettuali concrete. Attraverso tecniche di *whiteboarding*, *information mapping* e *co-design* collaborativo, sono stati rielaborati i contenuti del Regolamento, organizzandoli in un'architettura chiara, coerente e facilmente fruibile. La terza fase è stata invece dedicata alla "Prototipazione" (sezione 2.3) della soluzione scelta, che ha assunto la forma di un documento interattivo a contenuto visivo e testuale, coerente con la logica della conformità alla normativa. Le disposizioni del regolamento, nonché i requisiti essenziali di natura tecnico-informatica, sono stati rielaborati e sintetizzati in schemi e percorsi visuali che consentissero una

5. Mantelero–Vaciago–Esposito–Monte 2020.

6. Si veda, *ex multis*, Rossi–Palmirani 2020; Rundle 2006; Garante per la Protezione dei Dati Personali 2025.

7. Lewrick–Link–Leifer 2018; Lewrick–Link–Leifer 2020. Si veda anche Ducato–Strowel 2021.

comprensione immediata e funzionale dei relativi obblighi. Successivamente, nella quarta fase, "User test" (sezione 2.4), sono stati coinvolti nuovi soggetti dai diversi *background* (es., consulenti tecnici; giuristi; informatici; responsabili aziendali) al fine di testare il prototipo e valutare l'efficacia comunicativa e la fruibilità operativa. I feedback raccolti, sia sul piano percettivo-visivo, sia concettuale-logico, hanno consentito di apportare le necessarie modifiche e ottimizzazioni in vista del rilascio definitivo della Guida. Infine, nella quinta fase, "Miglioramento & Lancio" (sezione 2.5), sono state apportate le modifiche necessarie alla luce dei feedback emersi nella fase precedente e quindi è stato organizzato il rilascio della Guida.

La Guida è stata progettata e sviluppata nell'ambito del progetto "EcoCyber – Risk Management for Future Cyber-Physical Ecosystems", realizzato all'interno della Partnership Estesa SERICS (PE00000014), che è un'iniziativa nazionale del Piano Nazionale di Ripresa e Resilienza (PNRR) del MUR, finanziata dall'Unione Europea – Next Generation EU. Il progetto EcoCyber è dedicato allo sviluppo di soluzioni e metodi tecnici e giuridici innovativi per sfruttare le opportunità offerte dai sistemi cyber-fisici, affrontando al contempo le sfide connesse (ad esempio, minacce e vulnerabilità informatiche). In particolare, questo lavoro è stato condotto dai team di ricerca di due Work Package di EcoCyber: WP 2 – Soluzioni per la progettazione e il collaudo di componenti smart sicuri e WP 4 – Regole per la società del futuro, integrando così gli aspetti tecnici e legali nel summenzionato approccio multidisciplinare[8].

2. Realizzazione della Guida

I motivi per i quali si è deciso di concentrare la Guida sul regolamento Cyber Resilience Act sono duplici. Al fine di risolvere la frammentazione del quadro normativo europeo in materia di cybersicurezza in relazione alla generalità dei prodotti hardware e software[9], il regolamento introdurrà una nuova serie di requisiti tecnici "di cybersicurezza di base" ed obblighi giuridici ad un ampio novero di soggetti privati che intendono immettere sul mercato unico "prodotti con elementi digitali"[10]. Connesso a ciò, l'intrinseca combinazione di elementi tecnici e giuridici, propria della legislazione armonizzata in materia di sicurezza dei prodotti[11], rende il CRA un atto giuridico ad alta complessità[12].

Combinando due approcci regolatori distinti, quello della sicurezza dei prodotti e quello basato sul rischio, il CRA introduce requisiti essenziali di cybersicurezza vincolanti per l'immissione sul mercato di prodotti con elementi digitali, un aspetto finora disciplinato solo attraverso pratiche volontarie di settore o accordi contrattuali tra operatori economici. I requisiti essenziali sono prescrizioni di alto livello; con il cd. "Nuovo

8. Coordinati rispettivamente dai professori Marco Prandini (DISI-Unibo) e Raffaella Brighi (DSG-Unibo).
9. Il quadro giuridico dell'Ue in materia di cybersicurezza antecedente al CRA si concentrava infatti su settori specifici o categorie di prodotti delimitate, lasciando pertanto scoperta una vasta parte del mercato digitale. Se il Regolamento (UE) 2019/881 (Cybersecurity Act) ha introdotto un sistema di certificazione per prodotti, servizi e processi ICT, caratterizzato pertanto dalla volontarietà, i soli requisiti obbligatori in materia di cybersicurezza per prodotti con elementi digitali erano frammentati tra diversi atti giuridici, in base al settore o alla categoria di prodotto. Ad esempio, la direttiva 2014/53/UE (direttiva sulle apparecchiature radio), anche e soprattutto attraverso il regolamento delegato (UE) 2022/30, impone requisiti di cybersicurezza limitati ai prodotti elettrici o elettronici che emettono e/o ricevono intenzionalmente onde radio, lasciando pertanto fuori dall'ambito di applicazione tutti i prodotti connessi per altro mezzo che non fossero le onde radio. Ancora, il regolamento (UE) 2017/745 stabilisce *inter alia* requisiti di cybersicurezza per i soli dispositivi medicali.
10. L'ambito di applicazione oggettivo del CRA include i prodotti con elementi digitali messi a disposizione sul mercato la cui finalità prevista o il cui utilizzo ragionevolmente prevedibile include una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete (art. 2, para. 1), dove per "prodotto con elementi digitali" si intende qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware immessi sul mercato separatamente (art. 3, punto 1).
11. Commissione europea 2022.
12. Teichmann–Sergi 2025, p. 7.

Approccio" del 1985, confermato dal "Nuovo Quadro Legislativo" del 2008, i requisiti essenziali sono dettagliati dalle norme armonizzate europee, vale a dire standard tecnici elaborati dagli organismi di normazione europei (CEN, CENELEC, ETSI) dietro mandato della Commissione ed adottati da quest'ultima[13].

I requisiti essenziali, unitamente a diversi obblighi degli operatori economici rilevanti lungo l'intera catena di valore dei prodotti (fabbricanti, ma anche distributori, importatori, rappresentanti autorizzati), si estendono per l'intero ciclo di vita del prodotto, imponendo misure di sicurezza by design e by default, gestione delle vulnerabilità, aggiornamenti, e documentazione tecnica continua. Secondo l'approccio *risk-based*, invece, i prodotti sono classificati in base al livello di rischio di cybersicurezza, con la conseguenza di avere procedure di valutazione della conformità differenziate a seconda del grado di rischio (dall'autovalutazione al controllo da parte di organismi notificati). L'interazione tra questi due modelli genera un sistema complesso, in cui le imprese devono integrare competenze normative e tecniche per interpretare correttamente obblighi variabili e nuovi, gestire rischi dinamici e garantire la conformità durante tutta la vita del prodotto.

Avendo scelto di adottare la tecnica del legal design per rendere più agevole l'interpretazione non solo delle disposizioni giuridiche, ma anche, e soprattutto, dei meccanismi tecnico-giuridici del regolamento, con l'obiettivo di supportare gli operatori nei processi di conformità, la prima questione di design affrontata è stata come rappresentare graficamente in modo chiaro e intuitivo tali contenuti, mantenendo al tempo stesso il rigore e la precisione del testo normativo[14]. Infatti, per quanto l'idealtipo di destinatario della Guida sia un tecnico professionista, sia nell'ambito legale che in quello informatico, l'intento che ha animato la traduzione e riformulazione del regolamento in componenti visive e grafiche è stato quello di rendere più chiara la lettura e la comprensione del testo giuridico anche all'utilizzatore che non dispone necessariamente degli strumenti ermeneutici del tecnico.

Nel contesto della progettazione dell'informazione, e quindi della grafica e delle interfacce, il problema della comunicazione mediata assume un rilievo peculiare allorché le azioni poste in essere dall'utente, sulla base della propria interpretazione dell'artefatto, possano produrre effetti giuridicamente rilevanti[15]. La mediazione visiva non si limita a svolgere una funzione estetica o divulgativa, ma incide direttamente sui processi cognitivi e decisionali che presiedono alla comprensione e all'applicazione della norma. La questione si pone dunque in termini di responsabilità progettuale: il design dell'informazione giuridica deve garantire, oltre alla chiarezza comunicativa, anche la fedeltà concettuale e sistematica rispetto al contenuto normativo di riferimento[16].

Al tempo stesso, è opportuno precisare che la Guida non si configura come un processo di "iconizzazione" di disposizioni giuridiche, operazione che potrebbe introdurre criticità in ordine alla qualità e all'affidabilità della rappresentazione normativa, bensì come una traslazione grafica strutturata e analitica del testo giuridico. Tale impostazione metodologica mira a preservare, da un lato, la coerenza semantica e sistematica della disposizione e, dall'altro, ad evitare un'eccessiva semplificazione che possa compromettere l'accuratezza interpretativa del dato normativo. In questo senso, la rappresentazione visuale non sostituisce la norma, ma ne costituisce una diversa forma di accesso e comprensione, fondata su criteri di rigore, trasparenza e conformità giuridica.

2.1. Ricerca

Dopo aver delineato l'oggetto e gli obiettivi del progetto, nella prima fase, ancora in uno stadio preliminare, abbiamo individuato chi fossero i soggetti maggiormente interessati alla Guida. I destinatari primari sono stati individuati tra le aziende rientranti nell'ambito di applicazione del regolamento. Destinatari secondari della Guida sono stati identificati negli esperti del diritto (es., avvocati) ed

13. Kamara 2025.
14. Rossi–Haapio 2019. Si veda anche Ducato–Strowel 2021.
15. Rossi–Palmirani 2020.
16. Perondi 2024.

informatici che avrebbero dovuto studiare il regolamento per supportare le attività di conformità degli operatori economici destinatari degli obblighi del CRA. L'obiettivo di questa prima attività era pertanto comprendere l'approccio specifico dei diversi soggetti aziendali coinvolti nella compliance normativa, le principali criticità riscontrate di fronte a nuove normative e i bisogni informativi che sono emersi nella specifica fase di adeguamento al CRA[17].

Dopo aver definito un numero congruo di partecipanti (5 aziende e/o professionisti operanti sul territorio nazionale), abbiamo somministrato loro un'intervista strutturata, composta da 21 domande, divise in 6 sezioni con allegata l'informativa sul trattamento dei dati personali ai sensi degli artt. 13 e 14 GDPR. Nelle prime due sezioni le domande hanno preso in esame, da una parte, il contesto specifico dell'intervistato[18] e, dall'altra, le modalità con le quali gli intervistati approfondiscono una normativa[19]. La terza sezione ha poi definito il perimetro delle attività progettuali indagando il grado di conoscenza e approfondimento del CRA[20]. In questo contesto, la quarta sezione ha verticalizzato il focus sulla complessità delle attività interpretative e su determinati casi-limite[21]. La quinta sezione, invece, ha preso in esame la relazione tra il CRA e le altre normative di settore[22]. La sesta sezione si è infine concentrata sui risultati attesi da parte dei partecipanti all'intervista dal progetto "Guida

17. Così Hagan 2020, p. 8-9: "the goal is to find people in the context of the system [nel nostro caso, il CRA, ndr.] who are trying to use the system through its technologies, rules, interfaces, language, and services and then to gather information from them by triggering a reflective process that can expose what their deeper needs and aspirations are".
18. È stato chiesto quale fosse il ruolo attuale e in che modo l'intervistato, unitamente al team di appartenenza, fosse coinvolto nella normativa in azienda; quali fossero i team o singoli professionisti all'interno dell'azienda che si occupano a vario titolo delle attività di progettazione, sviluppo e conformità del prodotto rispetto alla normativa e con i quali l'intervistato si interfaccia ogniqualvolta si debba applicare un nuovo perimetro normativo; una descrizione, per punti o fasi, del flusso di consegne/lavoro tra i team di lavoro coinvolti nelle attività di compliance normativa.
19. È stato chiesto quali fossero le principali fonti utilizzate per l'interpretazione delle disposizioni normative; come queste fossero state reperite e quali fossero state giudicate le più complete e funzionali. Inoltre, è stato chiesto quali fossero i criteri per la selezione di professionalità per la soluzione di dubbi interpretativi.
20. È stato chiesto agli intervistati se avessero già approfondito il CRA in vista della sua applicazione; se, oltre al testo del regolamento, avessero consultato materiali di supporto per comprenderlo meglio (es., sintesi, schede pratiche, guide, ecc.), e, in caso di risposta affermativa, quali avessero trovato più chiari e utili. Infine, è stato chiesto agli intervistati di riordinare alcuni elementi centrali della normativa (es., data di entrata in applicazione; ambito di applicazione; obblighi per i soggetti; procedure documentali; casi limite ed esempi pratici; glossario tecnico e definizioni chiave; procedure di valutazione della conformità; sanzioni) in base all'ordine di priorità data all'elemento normativo-informazionale, immaginando di consultare una "guida al CRA".
21. È stato chiesto agli intervistati quali parti del CRA ritenessero più complesse da interpretare o applicare (ad es., definizioni, ambito di applicazione, criteri per "prodotto con elementi digitali"); se avessero già effettuato una valutazione per identificare quali, tra i loro prodotti, rientrassero nello *scope* del regolamento e se, contestualmente, fossero emersi casi-limite in cui non fosse chiaro se un prodotto con elementi digitali fosse soggetto al CRA. Connesso a ciò, è stato chiesto agli intervistati quali figure e ruoli, all'interno del contesto aziendale, fossero coinvolte nella decisione finale sul fatto che un prodotto debba essere conforme al regolamento. Sotto altro profilo, gli intervistati hanno indicato quali aspetti del regolamento generassero le maggiori difficoltà operative per le organizzazioni di riferimento (es., produzione della SBOM; gestione degli aggiornamenti di sicurezza; gestione delle vulnerabilità; ecc.).
22. È stato chiesto agli intervistati se, rispetto alla documentazione tecnica richiesta già da altre normative applicabili (es. direttiva RED, direttiva NIS2, AI Act, ecc.), avessero chiaro come integrare i requisiti del CRA e se, in questo contesto, ritenessero che il CRA si sovrapponga o entri in conflitto con altre normative applicabili ai prodotti forniti oppure se, di contro, rilevassero sinergie sfruttabili.

al CRA"[23]. Una domanda di chiusura della *survey*[24] ha chiesto agli intervistati se non avessimo incluso tra le domande degli elementi che, secondo loro, sarebbero stati utili per capire meglio i problemi applicativi del CRA nei loro contesti aziendali.

Dall'indagine è emerso che tutti gli intervistati hanno già intrapreso le attività di approfondimento sul CRA, sebbene con diversi gradi di dettaglio. Rispetto alle fonti utilizzate, prevalgono i materiali ufficiali (es., testo del regolamento sulla Gazzetta Ufficiale dell'Ue) e solo secondariamente workshop, webinar e sintesi di consulenti esperti. Con riferimento a questi materiali di supporto, un partecipante segnala la scarsa applicabilità di tali risorse, giudicate "troppo poco chiare" e "lontane dalla realtà operativa".

Quando invitati a ordinare le sezioni di una potenziale guida al CRA secondo priorità di consultazione, i partecipanti convergono su una struttura orientata agli aspetti pratici e applicativi. Le aree ritenute più rilevanti sono: (i) data di entrata in vigore e tempistiche di applicazione; (ii) obblighi per i soggetti coinvolti; (iii) procedure documentali e operative; (iv) ambito di applicazione del regolamento. Seguono, in ordine decrescente, le sezioni relative alle procedure di valutazione, ai casi-limite ed esempi pratici, e solo successivamente alle definizioni o ai glossari tecnici.

In ordine invece alle principali difficoltà di interpretazione, alcuni degli intervistati ritengono che l'ambito di applicazione, nonché i criteri di classificazione dei prodotti siano troppo ambigui; ulteriore criticità emersa è la gestione di componenti di terze parti, soprattutto nei casi in cui non sia possibile ottenere collaborazione dai fornitori, nonché la traduzione delle prescrizioni normative in soluzioni tecniche praticabili nei diversi contesti (software, macchinari industriali, sistemi IoT). A livello operativo, le problematiche più ricorrenti si concentrano sulla gestione degli aggiornamenti di sicurezza e sul monitoraggio delle vulnerabilità e degli incidenti, seguiti dalla gestione documentale e dall'eventuale produzione della *Software Bill of Materials* (SBOM)[25].

Per quanto concerne invece lo stato di implementazione del CRA, tre organizzazioni hanno già completato una valutazione interna per determinare i prodotti soggetti al regolamento; i cd. "casi-limite" (difficoltà nel determinare l'applicabilità del regolamento ad un dato prodotto con elementi digitali) sono al momento poco frequenti. In questo contesto, le figure coinvolte nelle decisioni legate alla compliance variano sensibilmente tra le organizzazioni: in alcuni casi la responsabilità è affidata all'ufficio legale o alla direzione, in altri al CTO, ai referenti di progetto o a consulenti esterni.

Sul piano normativo, emerge una percezione diffusa di una parziale sovrapposizione con la direttiva NIS2, ma non di conflitto. Alcuni partecipanti segnalano possibili sinergie operative, in particolare nella gestione degli accessi e dei log. Solo due organizzazioni dichiarano di avere già chiaro come integrare i requisiti del CRA con quelli di normative esistenti (es., direttiva sulle apparecchiature radio [RED][26], AI Act, MDR), mentre le altre sono ancora in fase di analisi.

Infine, tutti i partecipanti concordano sull'utilità di una *guida operativa* che semplifichi il CRA attraverso schemi, elementi grafici e strumenti pratici. Gli strumenti ritenuti più utili, in ordine di priorità, sono: (i) flowchart decisionali per determinare l'ambito di applicazione e le classi di rischio; (ii) checklist operative per verificare la conformità dei prodotti e dei processi; (iii) template documentali

23. È stato chiesto agli intervistati se potesse essere utile per le attività di compliance un documento-guida che diminuisse la complessità del regolamento anche attraverso l'introduzione di elementi grafici-schematici e come loro immaginassero tale output (es., flowchart decisionali; tabelle di confronto; checklist operative; template di documenti; glossario visuale; struttura logica e ragionata degli articoli del regolamento; ecc.). In conclusione, gli intervistati hanno dovuto indicare eventuali esempi di guide simili che avessero trovato particolarmente utili.

24. Lewrick–Link–Leifer 2018; Lewrick–Link–Leifer 2020.

25. Si veda, ad esempio, nel contesto nazionale, l'adozione del framework CycloneDX, versione 1.6, attraverso le linee guida pubblicate da ACN a fine ottobre 2025, nel contesto dell'applicazione dei criteri di premialità di cui all'articolo 14 della legge n. 90/2024. Il DPCM 30 aprile 2025, in attuazione dell'articolo 14 della legge 90/2024, prevede all'articolo 4 l'applicazione dei sopra citati criteri di premialità, "previa analisi dell'elenco di tutti i componenti di fabbricazione del prodotto o delle infrastrutture impiegate per erogare un servizio" (*bill of materials*).

26. Sulla relazione tra cybersicurezza e direttiva RED, si permetta di rimandare a Chiara 2022.

per la dichiarazione di conformità e la reportistica; (iv) esempi di casi-limite e tabelle di confronto tra normative; (v) struttura logica e ragionata del CRA per orientarne la lettura.

Nessuno dei partecipanti ha citato strumenti esistenti ritenuti chiari o completi, confermando una lacuna di risorse di riferimento a livello europeo e nazionale.

2.2. Definizione & Ideazione

La mancanza di linee guida operative, che adottino un linguaggio semplice, di un regolamento ad alta complessità tecnico-giuridica come il CRA è una delle principali problematiche evidenziate dagli operatori economici emerse nell'analisi empirica. Pertanto, per produrre la Guida al CRA, la seconda fase progettuale è coincisa con la delimitazione dell'obiettivo progettuale. In particolare, sono stati individuati non solo i nuclei concettuali centrali del Regolamento, ma anche i meccanismi tecnici e gli istituti giuridici più "critici", al fine di chiarire la struttura tecnica-organizzativa del CRA, percepita, soprattutto in specifici articoli, come troppo intricata. In particolare, le norme afferenti a un medesimo tema risultano spesso distribuite in più punti del Regolamento, ovvero tra i paragrafi di un singolo articolo e attraverso i continui rinvii ai diversi articoli e allegati. In questo modo, specifiche informazioni e procedure, seppure concettualmente e operativamente connesse, risultano distanti nella struttura formale, sfuggendo così a una chiara visione d'insieme.

Tale attività si è concentrata sui primi tre capi del regolamento, insieme alle regole sulle sanzioni contenute nel capo VII, in quanto definiscono i requisiti e gli obblighi che incidono direttamente sul modo in cui il regolamento deve essere compreso e attuato dagli operatori economici. Pertanto, l'attività di mappatura non ha ricompreso il capo IV del CRA, che introduce regole per le autorità nazionali responsabili degli organismi di valutazione della conformità (organismi notificati), e non quindi requisiti ed obblighi direttamente rivolti agli operatori destinatari della Guida.

Il testo del Regolamento, una volta rielaborato, è stato oggetto di una mappatura[27] su whiteboard, vale a dire di una scomposizione, o vero e proprio "spacchettamento", in macrosezioni, all'interno delle quali gli articoli afferenti a uno stesso sub-argomento sono stati organizzati in flussi caratterizzati da un preciso ordine e consequenzialità logica (Figura 1[28]), evidenziando non solo la struttura concettuale, ma anche le dinamiche semantiche del testo normativo.

Si è infatti lavorato su un duplice piano: da un lato, la razionalizzazione logica dei contenuti, finalizzata a rendere chiara la relazione tra norme, allegati e rimandi interni; dall'altro, una analisi linguistico-giuridica puntuale, che ha consentito di individuare e valorizzare tutti gli elementi lessicali con funzione condizionale o limitativa (ad esempio, *where*, *only when*, *provided that*, *may*, *shall be*) e di riconoscerne il peso specifico, in termini giuridici, ponendoli nella stessa mappa come punti di attenzione e "nodi semantici" di ulteriori diramazioni di flussi (Figura 2).

Al contempo, sono state ideate potenziali soluzioni visuali di raggruppamento dei contenuti e sono state identificate le corrispondenti etichette tematiche. In parallelo, sono stati tracciati tutti i rimandi e le connessioni trasversali tra gli articoli e gli allegati, propedeutici alla costruzione di un prototipo che garantisse una fluida navigazione e una comprensione sistemica dell'intero Regolamento.

In questa fase si è quindi materialmente definita la struttura portante del successivo prototipo, una "visione satellitare" del Regolamento finalizzata a garantire, a diverse altezze, coerenza testuale e architettonica. Macroscopicamente, dunque, si è perseguita l'ambizione di restituire linearità e chiarezza, al fine di predisporre un format che risultasse quanto più possibile coerente, accessibile e rispondente alle diverse esigenze di fruizione.

Ad esempio, l'articolo 13 rappresenta una delle disposizioni più dense, complesse e centrali dell'intero Regolamento. Nei suoi 25 paragrafi, infatti, racchiude e dettaglia gli obblighi che i fabbricanti (utenti primari di progetto) devono adempiere per garantire la conformità dei propri prodotti ai sensi

27. Lewrick–Link–Leifer 2018; Lewrick–Link–Leifer 2020.

28. Le figure nel contributo hanno scopo puramente esplicativo della metodologia adottata. Per approfondimenti relativi ai contenuti si rimanda alla consultazione della Guida, scaricabile in PDF dal sito https://site.unibo.it/cybersecurity-legal-lab.

del Regolamento. Tale norma risulta di difficile lettura in diversi punti, sia per la complessità lessicale e sintattica del testo normativo, sia per la distribuzione frammentata al suo interno e negli allegati.

Al fine di ridurre la complessità dell'articolo 13, il lavoro si è pertanto concentrato sul "riordinare" i diversi obblighi dei fabbricanti secondo un criterio logico-procedurale, costruito riflettendo in modo funzionale il ciclo di attività e adempimenti che l'operatore è tenuto a rispettare. In particolare, gli obblighi sono stati suddivisi nelle tre fasi caratteristiche del processo della conformità nell'ambito della legislazione armonizzata: (i) pianificazione, design, sviluppo, produzione; (ii) messa a disposizione sul mercato; (iii) periodo di assistenza. È stato inoltre aggiunto un livello ulteriore, trasversale alle tre fasi, contenente gli obblighi che i fabbricanti devono osservare in tutte e tre le fasi precedenti, quindi costantemente durante l'intero ciclo di vita del prodotto.

Come illustrato nella Figura 3, tutti i 25 paragrafi dell'articolo sono stati inizialmente "scorporati" e trasposti in un elenco consequenziale verticale (in verde), consentendo una lettura analitica e ordinata del testo normativo. Questa prima fase di scomposizione ha permesso di accompagnare la segmentazione con una parallela analisi del linguaggio giuridico, evidenziando ridondanze, ripetizioni e rimandi interni che ostacolavano la chiarezza. Successivamente, si è proceduto a un'opera di riorganizzazione in forma visiva (Figura 4): i paragrafi dell'articolo sono stati etichettati in base al tema specifico di riferimento (es., obblighi documentali, gestione delle vulnerabilità, periodo di supporto, informazioni da notificare alle autorità, informazioni da notificare agli utenti) e collocati all'interno di uno schema grafico che riproduce le tre fasi del ciclo di vita dei prodotti con elementi digitali. In tal modo, ciascun obbligo è stato "posizionato" nella fase procedurale in cui il fabbricante è tenuto ad adempiervi, rendendo immediatamente percepibile la sequenza logica e temporale delle attività richieste. Nella parte superiore dello schema, invece, è stata aggiunta una porzione di tabella dedicata ai paragrafi i cui obblighi devono essere adempiuti dai fabbricanti in modo continuativo durante tutto il ciclo di vita del prodotto (in azzurro).

In tal modo, l'approccio di legal design, coadiuvato dalla competenza tecnico-giuridica, ha permesso non solo di implementare una rappresentazione visiva chiara e immediatamente leggibile dell'articolo, ma anche di trasformare il testo normativo in uno strumento operativo, sempre tecnicamente corretto, capace di rappresentare il flusso degli adempimenti in modo coerente con la sequenza reale delle attività che i fabbricanti sono chiamati a svolgere.

Come ricordato supra, il CRA stabilisce dei requisiti essenziali di cybersicurezza, i quali coprono le tematiche di sicurezza del prodotto e i processi di gestione delle vulnerabilità. Tali requisiti devono essere implementati dai soggetti ricadenti nell'ambito di applicazione del CRA al fine di garantire un adeguato livello di cybersecurity per i prodotti con elementi digitali che essi sviluppano.

Dal punto di vista tecnico ed ingegneristico, il progetto si è confrontato con la necessità di rendere maggiormente chiari e dettagliati i ventuno requisiti essenziali di cybersecurity del CRA, necessariamente formulati in modo generico e poco operativo, e che non hanno ancora ricevuto un'adeguata implementazione tecnica attraverso il previsto rilascio delle norme tecniche armonizzate. A tal fine, è stata effettuata un'attività di mappatura degli standard tecnici esistenti, a livello internazionale ed europeo, al fine di valutare la copertura da loro offerta ai requisiti del CRA, facilitando così le procedure di conformità al regolamento, nelle more delle norme tecniche armonizzate. Il punto di partenza di questa ricerca è stato un report dell'ENISA (Agenzia europea per la Cybersicurezza) del 2024[29]. Per ogni requisito, il report ENISA proponeva alcuni standard rilevanti, evidenziandone eventuali gap e limitazioni. Inoltre, definiva un set di sotto-requisiti per ognuno dei requisiti essenziali del CRA, finalizzati a dettagliarne ed espanderne le richieste in termini di specifiche di cybersicurezza.

Da una parte, l'attività progettuale ha analizzato ulteriori standard e sistemi di certificazione non ricoperti dalla mappatura ENISA; dall'altra, si è dettagliato il grado dell'indagine in un quadro analitico multilivello. Infatti, la realizzazione della componente tecnica della Guida è stata concepita come un processo sistematico, finalizzato a fornire

29. Joint Research Centre & ENISA 2024.

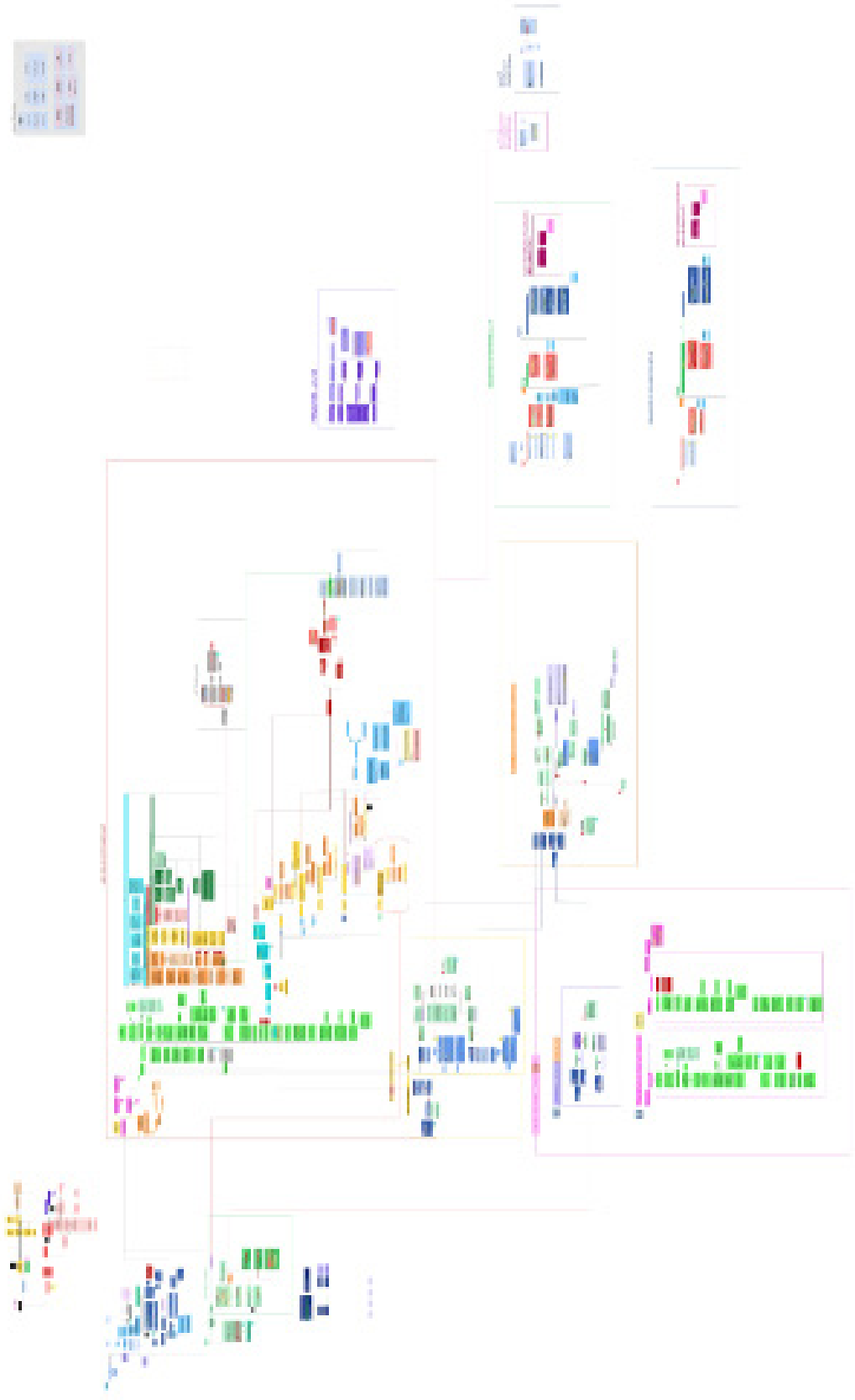

Fig. 1 — *Mappatura intera dei primi tre capi del Regolamento*

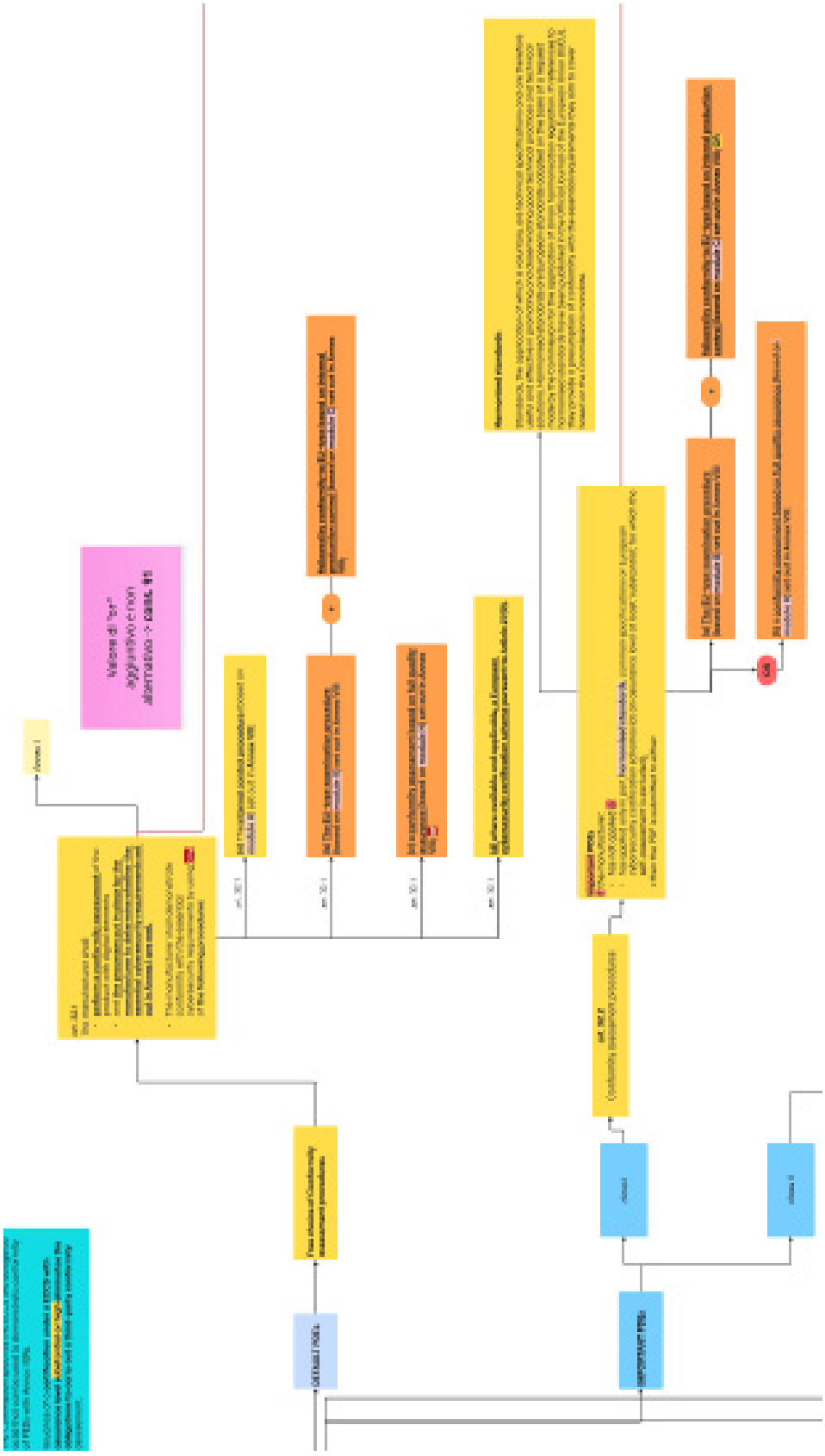

Fig. 2 — *Esempio di mappatura dei nodi semantici (Art. 32 – Procedure di valutazione della conformità)*

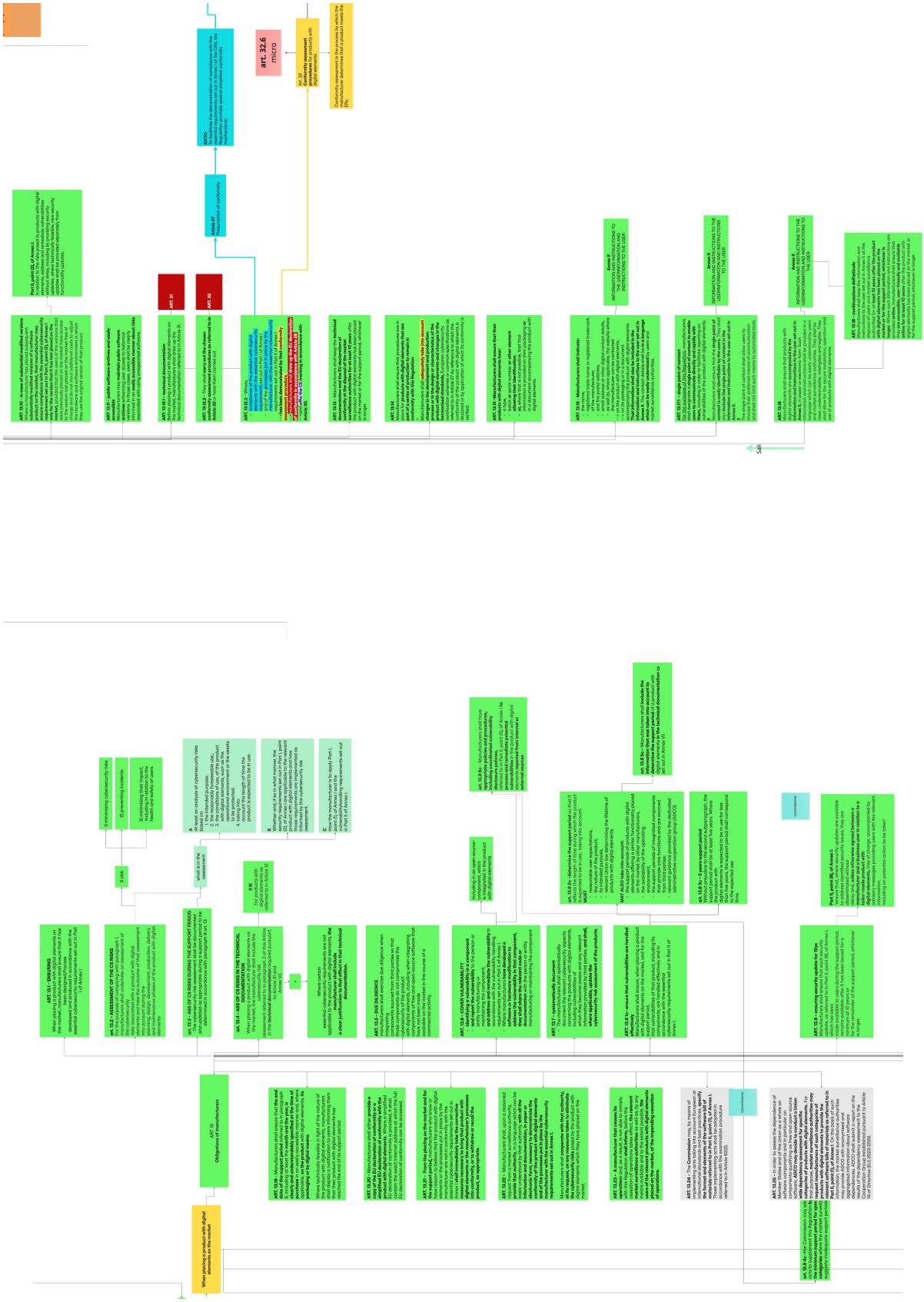

FIG. 3 — *Elenco consequenziale verticale di tutti i paragrafi dell'articolo 13*

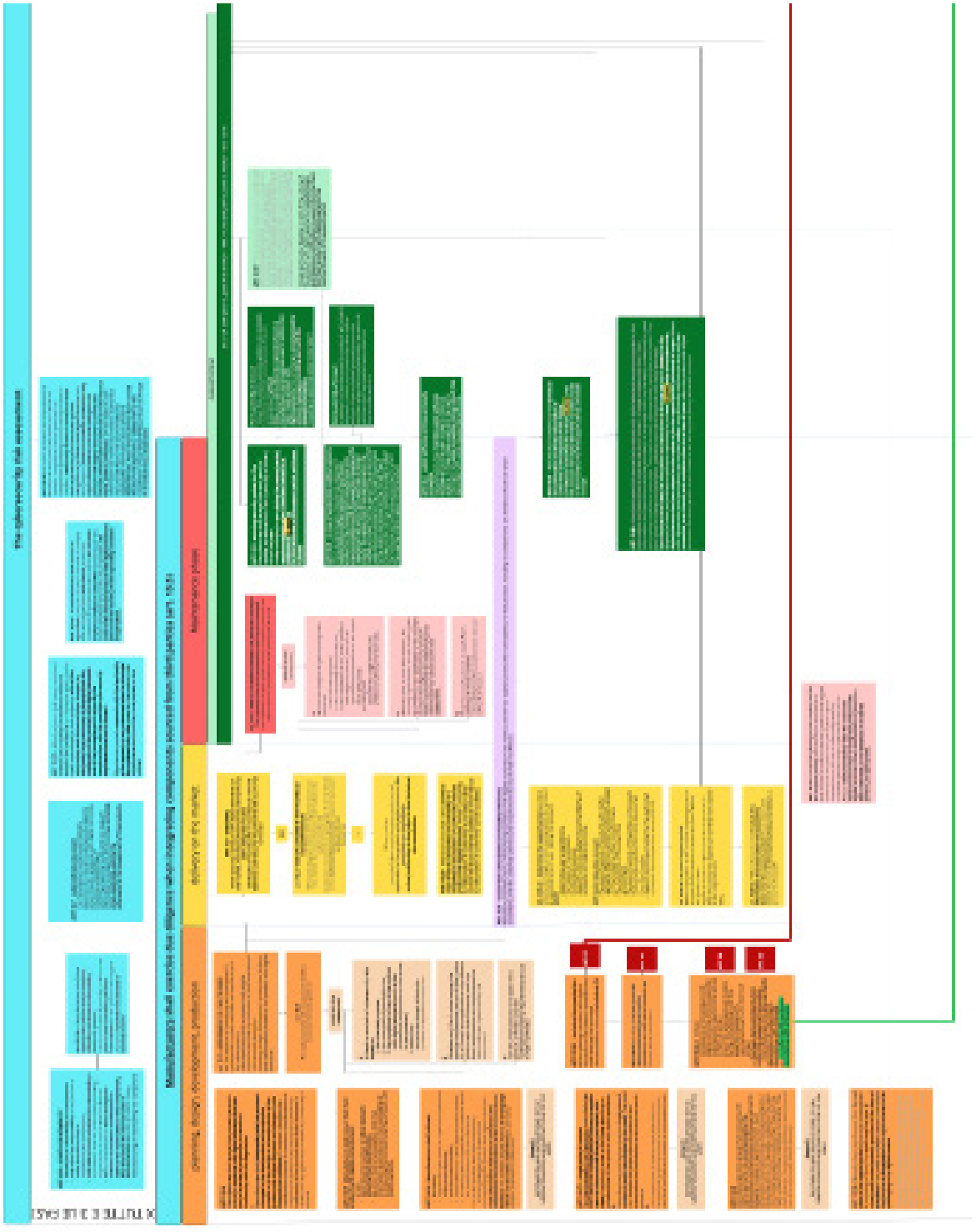

Fig. 4 — *Rappresentazione visiva, per fasi, dell'intero articolo 13*

una trasposizione operativa e strutturata dei requisiti del CRA in azioni concrete, tecnologie implementabili e riferimenti normativi ed istituzionali riconosciuti. L'obiettivo principale è stato quello di creare uno strumento di supporto pratico, ma al tempo stesso il più possibile rigoroso e completo, capace di tradurre la dimensione regolatoria del CRA in un insieme di attività tecniche e gestionali coerenti e immediatamente applicabili in contesti aziendali e industriali.

È necessario, tuttavia, notare che un corretto utilizzo della componente tecnica della Guida,

anche se completo ed esaustivo, non è da considerarsi come condizione sufficiente per raggiungere la conformità ai requisiti del CRA. Ai sensi dell'articolo 27 del Cyber Resilience Act, infatti, i prodotti con elementi digitali godono di una presunzione di conformità ai requisiti essenziali qualora rispettino gli standard armonizzati, le specifiche comuni adottate dalla Commissione attraverso atti di esecuzione, oppure siano certificati nell'ambito di schemi europei di certificazione della cybersicurezza. In attesa della pubblicazione di tali norme tecniche, i contenuti e le conclusioni presentati nel presente studio intendono contribuire al dibattito tecnico e scientifico che costituisce il fondamento del processo di standardizzazione e certificazione europea in materia di cybersicurezza.

In una prima fase, ogni requisito dell'Allegato I del CRA è stato analizzato e ampliato sulla base dei sotto-requisiti proposti da ENISA. Questo passaggio è stato fondamentale per garantire che la trattazione di ciascun requisito fosse completa, contestualizzata e coerente con le interpretazioni dell'Agenzia. A partire dai sotto-requisiti identificati, l'intero lavoro è stato organizzato secondo tre direttrici analitiche e complementari, che costituiscono la struttura portante della Guida dal punto di vista tecnico: 1. Attività & Principi; 2. Tecnologie & Strumenti; 3. Standard, linee-guida e migliori pratiche. Questa articolazione è stata progettata per rispondere alle diverse esigenze di chi, all'interno di un'organizzazione, si trova a dover implementare o supervisionare la conformità al CRA, dai profili manageriali ai tecnici operativi. La struttura tripartita della guida consente infatti di seguire un percorso logico e multilivello: il responsabile aziendale può individuare nella sezione "Attività e Principi" i processi necessari alla conformità; il team tecnico può approfondire la sezione "Tecnologie e Strumenti" per comprenderne le modalità di attuazione; infine, la sezione "Standard, linee-guida e migliori pratiche" permette di collocare le azioni intraprese all'interno di un quadro normativo di riferimento riconosciuto. In tal modo, la guida accompagna il lettore dal principio astratto (requisito essenziale) all'applicazione concreta, offrendo una visione completa e integrata dei requisiti del Cyber Resilience Act (Figura 5).

1) Attività e principi.

Relativamente alla prima direttrice, per ciascun requisito del CRA sono state individuate una serie di attività operative e di principi di sicurezza che un'organizzazione può mettere in atto per avvicinarsi alla soddisfazione dei vari requisiti. Ogni attività è formulata come un'azione operativa, ad esempio "Logging and Auditing" o "Authentication enforcement" o come principi di fondo, come il "Least Privilege", la "Defence-in-Depth" o il "Data Minimisation", fornendo una base teorica per la loro attuazione. Questa sezione consente quindi al lettore di identificare in modo immediato le azioni da intraprendere, costruendo una mappa chiara delle aree operative su cui intervenire per ciascun requisito normativo.

2) Tecnologie e strumenti.

La seconda direttrice, "Tecnologie e strumenti", traduce le attività precedenti in soluzioni pratiche e implementative. Per ogni attività individuata sono stati selezionati gruppi di tecnologie e strumenti da poter utilizzare al fine di implementare le attività proposte, fornendo anche esempi, ove possibile, di soluzioni open source. Questa scelta è motivata dal voler favorire la replicabilità e accessibilità delle soluzioni, dando modo al fruitore della guida di sperimentare strumenti spesso già ampiamente utilizzati, al fine di comprendere concretamente e tecnicamente le prescrizioni fornite dai requisiti del CRA. I gruppi di tecnologie sono organizzati per categoria funzionale (es. "Privileged Access Management solutions", "Host-based intrusion Detection systems", ecc.), in modo da consentire al lettore di poter individualmente approfondire le categorie ed individuare strumenti alternativi o complementari a seconda del proprio contesto operativo (IT, OT, IoT o embedded).

3) Standard, linee-guida e migliori pratiche.

La terza direttrice collega le due precedenti dimensioni operative al panorama normativo e regolamentare internazionale. Per ogni attività e requisito, la guida fornisce una selezione mirata di standard, framework e linee guida, scelte favorendo pubblicazioni di enti riconosciuti a livello internazionale ed europeo, quali ISO/IEC, NIST ed ENISA. Mentre il report ENISA fornisce principalmente riferimenti documentali relativi a noti standard pubblicati da ISO ed IEC, la Guida ha cercato di espandere questa sezione, includendo standard pubblicati da altri enti (es., NIST), oltre che citando migliori pratiche, linee-guida e framework in materia di cybersecurity (es., OWASP best

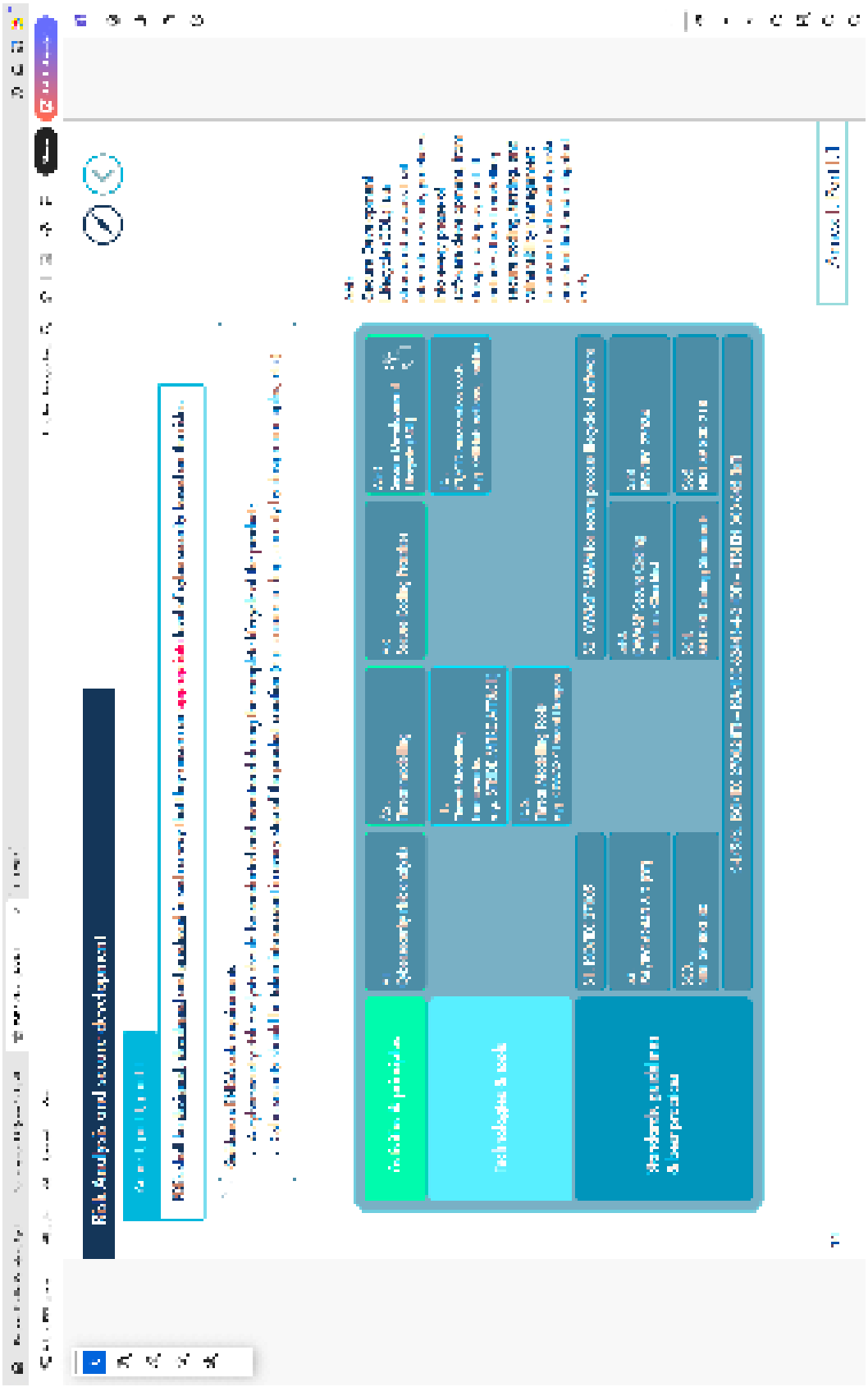

FIG. 5 — *Scheda sui requisiti essenziali ex Allegato I CRA*

practices, CIS benchmark), laddove ritenuti utili ai fini di una migliore comprensione dei requisiti del CRA. In particolare, sono stati analizzati nel dettaglio i requisiti (i.e., *Cybersecurity provisions*) proposti dalla versione 3.1.3 (la più recente a questa data) dell'ETSI EN 303 645, standard settoriale in materia di cybersicurezza per dispositivi IoT, e i requisiti (i.e., *Security practices*) definiti dalla versione 2 dell'OWASP SAMM, modello di maturità della sicurezza del software. Per ognuno dei requisiti definiti dagli standard citati, è stata identificata un'eventuale corrispondenza, forte o debole, con i requisiti del CRA, al fine di determinare standard specifici per vari settori (in questo caso rispettivamente IoT e sviluppo del software). Questo livello offre un fondamento normativo solido alle misure tecniche proposte, garantendo che siano in linea con gli standard internazionali più riconosciuti e fornisce al lettore un percorso di approfondimento autonomo, consentendogli di consultare le fonti ufficiali per estendere la propria conoscenza o per supportare futuri audit e processi di certificazione. La presenza di riferimenti incrociati, ad esempio tra *NIST SP 800-92* (per il log management) e *ISO/IEC 27002* (per i controlli di monitoraggio), permette inoltre di armonizzare il CRA con i framework esistenti, facilitando la convergenza tra compliance europea e standardizzazione globale.

2.3. Prototipazione

La rappresentazione grafica non ha seguito rigidamente l'ordine sistematico del regolamento, ma si è invece conformata a un criterio logico-procedurale di compliance, costruito attorno al ciclo di adempimento che l'operatore è tenuto a rispettare. Tale impostazione ha consentito di preservare la coerenza con la ratio e la struttura giuridica delle disposizioni, evitando al contempo una riproduzione meramente descrittiva del testo normativo[30]. Parallelamente, si è proceduto a un'ulteriore rifinitura dei testi, cioè un controllo terminologico e concettuale volto a garantire la fedeltà giuridica delle formulazioni, assicurando coerenza con la terminologia ufficiale del regolamento e con i principi generali del diritto dell'Unione europea in materia di armonizzazione tecnica e responsabilità degli operatori economici.

Così, riprendendo l'esempio dell'articolo 13 del regolamento, il prototipo della Guida ha tradotto graficamente il lavoro concettuale della precedente fase di mappatura. Come mostrato dalla Figura 6, la tavola racchiude al suo interno gli elementi ritenuti utili a orientare l'utente rispetto al frammento di regolamento oggetto di analisi. In alto a sinistra, la barra blu indica il *topic* specifico dell'articolo trattato, mentre nella parte inferiore destra lo stesso articolo è evidenziato per facilitarne il riconoscimento immediato. In alto a destra si trovano invece due strumenti di navigazione interattiva: l'icona color petrolio, che consente di tornare rapidamente all'ultima pagina visualizzata, agevolando la consultazione di sezioni correlate senza perdere la pagina di partenza; e l'icona blu, che permette di ritornare alla *dashboard* iniziale, una mappa dei contenuti del Regolamento, dalla quale è possibile accedere direttamente alle categorie, articoli o allegati di interesse. La parte centrale della tavola, che ne costituisce il fulcro visivo, è dedicata alla rappresentazione dell'articolo o di più articoli tra loro concettualmente connessi, riportati sempre sul margine sinistro. Questi sono affiancati, al centro, dai *box* contenenti il testo normativo, corredato da elementi grafici che ne facilitano la lettura lineare e la comprensione concettuale. All'occorrenza, sono state inserite anche icone segnaletiche che fungono da punti di attenzione, per evidenziare passaggi chiave contenuti nel testo normativo o peculiari procedure e adempimenti. I rinvii presenti nelle disposizioni analizzate all'Allegato I del regolamento, contenente i requisiti essenziali, sono rappresentati graficamente sotto forma di *box* che, se "cliccato", conduce all'apposita sezione nella Guida sui requisiti essenziali. L'uso dei colori, poi, è stato calibrato in modo pienamente funzionale alla comprensione cognitiva e intuitiva del contenuto: si è scelto, pertanto, di impiegare tinte distinte e non gradienti di una medesima palette, così da evidenziare visivamente le differenze concettuali e funzionali tra gli elementi rappresentati. Ad esempio, operando in questo senso, sono stati scelti tre colori nettamente differenti (rosso, verde, petrolio) per chiarire in quale delle tre fasi identificate sopra il singolo obbligo analizzato si trova. Con la stessa logica sono stati applicati i grassetti e gli evidenziatori cromatici per mettere in rilievo termini e

30. Koulu–Pohle 2024, p. 5.

locuzioni giuridicamente rilevanti, garantendo una lettura stratificata che agevola sia la consultazione esperta sia quella operativa.

La Figura 7 illustra come l'approccio metodologico adottato sia stato concretamente operazionalizzato nella Guida. Essa rappresenta un chiaro esempio del fatto che il lavoro di "ricomposizione" normativa non ha seguito una mera progressione numerica e sequenziale degli articoli o dei paragrafi, ma ha invece privilegiato una logica di flusso ragionato, capace di valorizzare la connessione funzionale tra gli obblighi previsti (vedi sezione 2.2). Come si evince dalla Figura, infatti, i paragrafi riportati non seguono l'ordine originario dell'articolo, ma vengono collocati in base alla fase (progettazione e sviluppo, immissione sul mercato, e mantenimento) in cui i relativi obblighi devono essere adempiuti. Tale rappresentazione, frutto di una lettura sistematica del testo giuridico e di una precisa disposizione cromatica e spaziale degli elementi, consente di visualizzare le relazioni logiche e temporali tra gli adempimenti, evidenziando al contempo le interdipendenze e i rimandi interni al Regolamento. In questo modo, la Guida consente di passare da una struttura normativa rigidamente testuale a una struttura cognitiva e processuale, che rispecchia la concreta sequenza di azioni e verifiche che i fabbricanti sono chiamati a svolgere.

Una critica che può essere mossa alla Guida, come ad altri progetti di legal design, è che una comunicazione grafica-visuale di contenuti giuridici potrebbe comportare il rischio significativo di non cogliere tutte le sfumature del discorso normativo[31]. Ciò, in particolare, per due ragioni. Da un lato, l'uso di tecniche di plain language[32] (volte a semplificare il linguaggio e a ridurre la densità sintattica) e, dall'altro, l'impiego di elementi grafici (come schemi, infografiche, icone o mappe concettuali) introducono un doppio livello di sforzo cognitivo per l'utente finale. Prima di poter accedere al contenuto, infatti, l'utente deve comprendere la logica strutturale e visiva dello schema, cioè il nuovo "modo di leggere" che esso impone, e solo successivamente può concentrarsi sul testo che vi è inserito. In questo processo, il rischio concreto è che alcune sfumature normative come rimandi, condizioni o relazioni tra disposizioni, non vengano pienamente colte: la mente, impegnata a decifrare la forma grafica, può distogliere attenzione dal contenuto giuridico, con la conseguenza di attenuarne o distorcerne il significato. Paradossalmente, quindi, un testo normativo privo di elementi grafici, e dunque più vicino a ciò che l'utente è storicamente abituato a leggere, ma rifinito attraverso sole tecniche di plain language, può costituire un intervento di legal design persino più efficace rispetto all'adozione estesa di componenti visuali.

Nel nostro lavoro, tuttavia, abbiamo scelto un approccio di equilibrio. Da un lato, l'intervento sul testo normativo è stato mirato: abbiamo operato soltanto nei passaggi che presentavano maggiore complessità sintattica (ad esempio, per la lunghezza dei periodi, l'uso di termini densi o di numerosi rimandi interni) evitando di sostituire integralmente il testo con una versione in *plain language*. Gran parte delle disposizioni è rimasta invariata, ove ritenuta già chiara e coerente con la terminologia e la logica del regolamento. Dall'altro lato, l'integrazione di schemi e altri elementi grafici è stata sempre accompagnata da una legenda esplicativa iniziale, volta a orientare l'utente nella lettura del modello visuale. Tale indicazione specifica come interpretare i diversi elementi grafici e logici, ricorrendo a strumenti di chiarezza percettiva (come grassetti, frecce, colori ben differenziati) per distinguere concetti, categorie e condizioni. Dunque, l'intento è stato quello di ridurre il carico cognitivo legato all'introduzione di una struttura visiva inedita, preservando al contempo la fedeltà giuridica, la precisione terminologica e una maggiore navigabilità dell'informazione normativa.

Inoltre, grazie alla fase di ricerca preliminare e, in particolare, ai risultati emersi dalla survey condotta sui destinatari del regolamento, è stato possibile mappare il percorso logico-pratico che gli utenti seguono per comprendere il nuovo testo normativo. Non sorprende che il regolamento rappresenti il primo punto di riferimento cui essi si rivolgono, al fine di acquisire un quadro istituzionale e completo del precetto normativo. Solo in un secondo momento gli utenti tendono a effettuare ricerche mirate presso fonti ed enti autorevoli, per ottenere chiarimenti operativi e guide interpretative che agevolino la corretta applicazione della normativa. In questo

31. Rossi–Palmirani 2020.

32. Ducato–Strowel 2021.

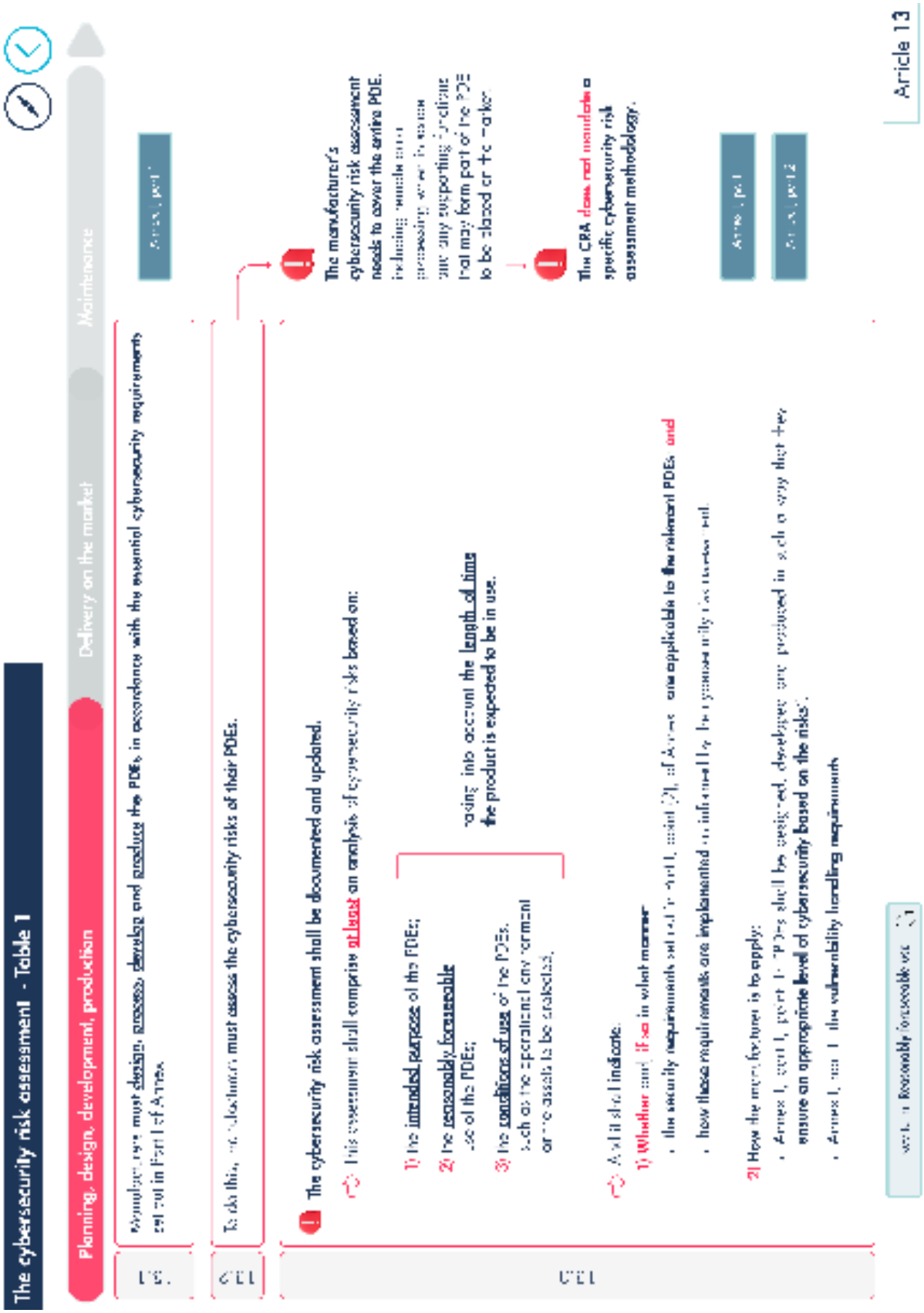

Fig. 6 — *Prima tavola articolo 13 CRA*

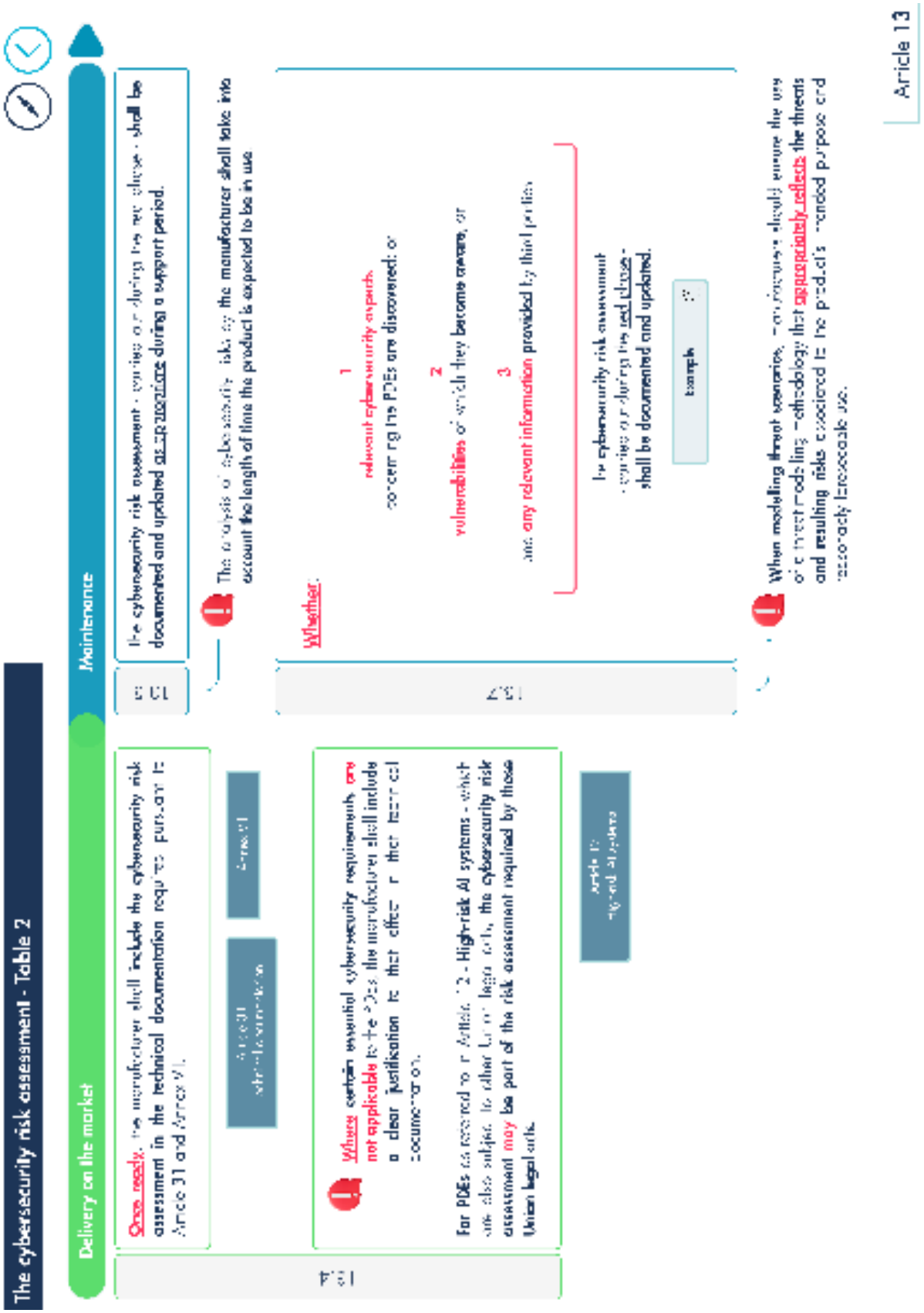

Fig. 7 — *Seconda tavola articolo 13 CRA*

senso, riteniamo che l'approccio da noi proposto non sia da intendersi in un'ottica di sostituzione del testo normativo, quanto di complementarietà[33]: gli elementi visuali della struttura compliance-friendly del regolamento, che evidenzia raccordi e sinergie tra disposizioni e meccanismi logicamente collegati (es., condizioni, criteri, ecc.), chiariscono e migliorano la fruibilità e navigazione dell'informazione contenuta nella norma[34].

2.4. User test

Questa fase ha previsto nuovamente il coinvolgimento dei soggetti che hanno partecipato alla survey nella prima fase, nonché di altri soggetti dalle diverse formazioni (es., consulenti tecnici; giuristi; informatici; responsabili aziendali), al fine di testare il prototipo, valutandone l'efficacia comunicativa e la fruibilità operativa. Questo passaggio di validazione empirica[35] basato sull'esperienza del settore privato è essenziale per evitare che la Guida diventi "solamente" un costrutto teorico privo di applicabilità pratica. I feedback raccolti, sia sul piano percettivo-visivo, sia concettuale-logico, hanno consentito di apportare le necessarie modifiche e ottimizzazioni in vista del rilascio definitivo della Guida.

2.5. Miglioramento & Lancio

In questa fase finale sono state apportate le modifiche necessarie alla luce dei feedback emersi nella fase precedente. Inoltre, sono state completate le attività necessarie al rilascio della Guida e alla sua diffusione, incluse la predisposizione di un sito web con dominio Unibo[36] dedicato al progetto che accoglie la Guida e la documentazione pertinente. Ancorché non sia formalmente richiesto dalla governance del Partenariato Esteso SERICS[37] che i prodotti della ricerca condotta all'interno dei progetti afferenti al Partenariato siano pubblicati in open access, la Guida è stata rilasciata in modalità aperta, con licenza CC-BY-NC-SA[38], per due ordini di ragioni. In primo luogo, riteniamo giusto che il prodotto di una ricerca finanziata con fondi pubblici sia liberamente disponibile alla collettività, in linea con i principi che sorreggono il movimento del libero accesso alla conoscenza[39]. In secondo luogo, la scelta dell'open access garantisce la massima diffusione e accessibilità della ricerca, permettendo pertanto la possibilità di raggiungere il più alto numero di destinatari della Guida (in particolare, gli operatori economici, molti dei quali potrebbero essere PMI). Connesso a ciò, per garantire una maggior diffusione dello strumento, la Guida è stata inizialmente prodotta in lingua inglese; peraltro, i fondi che hanno permesso lo sviluppo della Guida derivano da risorse finanziate dal piano dell'Unione europea Next Generation EU. In una fase successiva del progetto, è prevista una traduzione in italiano della stessa per un maggior allineamento al mercato nazionale. Un altro passaggio successivo al rilascio della Guida è legato alla sua trasformazione da file PDF interattivo a web tool interattivo, al fine di permettere una navigazione tra i contenuti più immersiva e intuitiva.

3. Conclusioni

Nel contesto attuale di "ipertrofia normativa" nell'ambito digitale[40], o di "tsunami di legislazione digitale"[41], le imprese sono sempre più destinatarie di oneri normativi e regolamentari, i quali

33. Ducato–Strowel–Marique 2024.
34. Perondi 2024.
35. Lewrick–Link–Leifer 2018; Lewrick-Link-Leifer 2020.
36. https://site.unibo.it/cybersecurity-legal-lab.
37. Decreto Direttoriale MUR, n. 1556 dell'11 ottobre 2022, con risorse a valere sull'Avviso Decreto Direttoriale 15 marzo 2022 n. 341, in attuazione dell'Investimento 1.3, finanziato dall'Unione europea - NextGenerationEU - nell'ambito della Missione 4 "Istruzione e ricerca" – Componente 2 "Dalla ricerca all'impresa" del Piano Nazionale di Ripresa e Resilienza.
38. Si veda nel sito di Creative Commons il codice legale della licenza Attribuzione – NonCommerciale - CondividiAlloStessoModo 4.0 Internazionale.
39. Caso 2022.
40. Papakonstantinou–De Hert 2024.
41. EDRi 2022.

risultano particolarmente costosi per le PMI[42]. I molteplici e diversi obblighi derivanti dalla regolamentazione del digitale di matrice eurounitaria (ma anche nazionale, in realtà) spesso risultano particolarmente complessi da tradurre in indicazioni operative per raggiungere il desiderato stato di conformità. Ciò è riconducibile non solo alla novità del perimetro normativo stesso, ma anche all'interazione tra l'elemento tecnico-giuridico e quello tecnico-informatico. Il regolamento europeo Cyber Resilience Act non è un'eccezione in tal senso. Anzi, ne costituisce forse la più chiara espressione.

La Guida al CRA qui presentata, con un'attenzione particolare soprattutto alla sua metodologia, alle varie fasi, cioè, che hanno costituito la sua ideazione e sviluppo, mira pertanto a risolvere le principali criticità interpretative dell'atto giuridico da parte degli operatori attraverso l'implementazione di principi e tecniche di legal design. Per quanto sia ancora prematura una valutazione in ordine all'impatto di tale strumento sul mercato, riteniamo che la diffusione e l'adozione di questa metodologia, e quindi per estensione di questi strumenti, possa rappresentare un elemento importante anche nell'ottica degli obiettivi di semplificazione della complessità (e quindi dei costi) della cd. "normativa digitale" dell'Ue, uno dei cardini politici del secondo mandato della presidente della Commissione europea Von der Leyen attraverso il cd. "pacchetto Omnibus"[43].

Riferimenti bibliografici

R. Caso (2022), *Open data, ricerca scientifica e privatizzazione della conoscenza*, in "Il Diritto dell'Informazione e dell'Informatica", 2022, n. 4-5

P. G. Chiara (2025), *Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?*, in "European Journal of Risk Regulation", vol. 16, 2025, n. 2

P.G. Chiara (2022), *Commission Delegated Regulation (EU) 2022/30 Supplementing Directive 2014/53/EU on Radio Equipment: Strengthening Cybersecurity, Privacy and Personal Data Protection of Wireless Devices*, in "European Data Protection Law Review", vol. 8, 2022, n. 1

Commissione europea (2025), *Omnibus package*, in "Simplifying the Single Market", single-market-economy.ec.europa.eu

Commissione europea (2022), *La guida blu all'attuazione della normativa UE sui prodotti 2022*, 2022/C 247/01

M. Draghi (2024), *The future of European competitiveness: a competitiveness strategy for Europe*, in commission.europa.eu, 2024

R. Ducato, A. Strowel (eds.) (2021), *Legal Design Perspectives. Theoretical and Practical Insights from the Field*, Ledizioni, 2021

R. Ducato, A. Strowel, E. Marique (eds.) (2024), *Design(s) for Law*, Ledizioni, 2024

EDRi (2022), *How it started, how it's going: Halfway through the current European Commission's legislative term*, in "edri.org", 2022

Garante per la Protezione dei Dati Personali (2025), *Rendere le informative privacy più chiare e rapidamente comprensibili – il Legal Design come approccio rivolto all'utente*, in "www.igsg.cnr.it", 2025

M. Hagan (2020), *Legal design as a thing: A theory of change and a set of methods to craft a human-centered legal system*, in "Design Issues", vol. 36, 2020, n. 3

42. Draghi 2024, p. 30 e 68-69.

43. Commissione europea 2025.

Joint Research Centre & ENISA (2024), *Cyber Resilience Act Requirements Standards Mapping*, Publications Office of the European Union, 2024

I. Kamara (2025), *Standardising personal data protection*, Oxford University Press, 2025

R. Koulu, J. Pohle (2024), *Legal Design Patterns: New Tools for Analysis and Translations Between Law and Technology*, in "Digital Society", vol. 3, 2024, n. 22

Legal Design Alliance (2018), *The Legal Design Manifesto v 1.0*, in "www.legaldesignalliance.org", 2018

M. Lewrick, P. Link, L. Leifer (2020), *The Design Thinking Toolbox. A Guide to Mastering the Most Popular and Valuable Innovation Methods*, Wiley, 2020

M. Lewrick, P. Link, L. Leifer (2018), *The Design Thinking Playbook. Mindful Digital Transformation of Teams, Products, Services, Businesses and Ecosystems*, Wiley, 2018

A. Mantelero, G. Vaciago, M.S. Esposito, N. Monte (2020), *The common EU approach to personal data and cybersecurity regulation*, in "International Journal of Law and Information Technology", vol. 28, 2020, n. 4

C.F. Mondschein (2016), *Some Iconoclastic Thoughts on the Effectiveness of Simplified Notices and Icons for Informing Individuals as Proposed in Article 12 (1) and (7) GDPR*, in "European Data Protection Law Review", vol. 2, 2016, n. 4

V. Papakonstantinou, P. De Hert (2024), *The Regulation of Digital Technologies in the EU: Act-ification, GDPR Mimesis and EU Law Brutality at Play*, Routledge, 2024

L. Perondi (2024), *La forma grafica del testo*, in B. Pasa, G. Sinni (a cura di), "Transparency by Design. Incontro interdisciplinare sul principio di trasparenza dei dati personali" (Venezia, 19 dicembre 2022), Bembo Officina Editoriale, 2024

A. Rossi, M. Palmirani (2020), *Can visual design provide legal transparency? The challenges for successful implementation of icons for data protection*, in "Design Issues", vol. 36, 2020, n. 3

A. Rossi, R. Ducato, H. Haapio, S. Passera (2019), *Legal Design Patterns: Towards A New Language for Legal Information Design*, in E. Schweighofer, F. Kummer, A. Saarenpää (eds.), "Internet of Things. Proceedings of the 22nd International Legal Infomatics Symposium IRIS 2019", Weblaw ed., 2019

A. Rossi, H. Haapio (2019), *Proactive Legal Design: Embedding Values in the Design of Legal Artefacts*, in E. Schweighofer, F. Kummer, A. Saarenpää (eds.) "Internet of Things. Proceedings of the 22nd International Legal Infomatics Symposium IRIS 2019", Weblaw ed., 2019

M. Rundle (2006), *International Personal Data Protection and Digital Identity Management Tools*, in "Berkman Center Research Publication" No. 2006–06, 2006

F. Teichmann, B.S. Sergi (2025), *The EU Cyber Resilience Act: Hybrid governance, compliance, and cybersecurity regulation in the digital ecosystem*, in "Computer Law & Security Review", vol. 59, 2025

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0238 • articolo sottoposto a peer review • pubblicato in anteprima il 25 set. 2025

Ernesto Ingenito

L'automazione dei processi nei contratti pubblici

Lo sviluppo dell'innovazione, al centro delle riforme e degli investimenti PNRR, ha indotto il legislatore a dedicare un ampio spazio al tema della digitalizzazione all'interno dell'impianto del nuovo Codice dei contratti pubblici. Il presente lavoro, più nello specifico, si focalizza sul riconoscimento – contenuto nell'art. 30 del citato Codice – a favore delle stazioni appaltanti e degli enti concedenti della possibilità di automatizzare le proprie attività ricorrendo a soluzioni tecnologiche con riguardo a tutto il ciclo di vita dei contratti pubblici. L'espressa apertura a soluzioni fondate su sistemi di intelligenza artificiale e di blockchain, ispirate al principio di buon andamento dell'azione amministrativa, induce a chiedersi quali siano effettivamente gli spazi che in questo settore ci saranno nel futuro prossimo per le nuove tecnologie. Per tale ragione, dopo aver analizzato i principi che orientano l'utilizzo di dette tecnologie e aver individuato i presidi imprescindibili che è necessario predisporre, occorre chiedersi quale tipologia di sistema fondato sull'intelligenza artificiale possa concretamente venire in rilievo e sotto quale profilo il settore dei contratti pubblici ne trarrà un beneficio. A tal fine si è ritenuto opportuno dare conto dei primi progetti pilota ideati e delle sperimentazioni che sono già state avviate.

Contratti pubblici – Intelligenza artificiale – Digitalizzazione – Blockchain – PNRR

Process automation in public procurement

Driven by the development of innovation, a key component of the reforms and investments promoted by PNRR (the Italian plan for economic recovery and resilience), the legislator has devoted considerable attention to digitalization within the framework of the new Public Procurement Code. This paper specifically focuses on Article 30 of the new Code, which explicitly allows contracting authorities and granting bodies to automate their activities using technological solutions throughout the entire lifecycle of public contracts. This formal endorsement of solutions based on artificial intelligence and blockchain technologies – framed by the principle of good administration – raises questions about the actual scope for adopting such technologies in this sector. Accordingly, after analysing the guiding principles for their use and identifying the essential safeguards to be implemented, the paper explores which types of AI systems may concretely apply and how public procurement could benefit. The analysis is supported by a review of early pilot projects and experimental initiatives already underway.

Public procurement – Artificial intelligence – Digitization – Blockchain – Next Generation EU

L'Autore è avvocato specializzato in diritto del lavoro, contratti pubblici, prevenzione della corruzione e nuove tecnologie

1. Introduzione

La rivoluzione tecnologica in atto e i processi di automazione che stanno interessando in maniera sempre più incisiva ogni campo del sapere hanno avuto delle ricadute drastiche anche sul mondo del diritto. Uno degli ambiti che in prospettiva è più interessato alla trasformazione digitale è sicuramente la contrattualistica pubblica laddove si consideri che il dichiarato invito – contenuto, come si vedrà in prosieguo, nel d.lgs. n. 36/2023 – rivolto alle stazioni appaltanti ad automatizzare le proprie attività deve essere declinato alla luce del principio del risultato di cui all'art. 1 del medesimo decreto e, più in generale, del principio di buon andamento della pubblica amministrazione di cui all'art. 97 Cost.[1]

Dopo aver passato in rassegna qual è la finalità della digitalizzazione delle procedure di gara e dell'intero ciclo dei contratti pubblici, appare di rilievo e, pertanto, meritevole di specifica attenzione il focus sui presupposti e i limiti entro cui si potrà ricorrere agli strumenti di automazione e, in particolare, all'intelligenza artificiale e alla blockchain.

Al riguardo non v'è dubbio alcuno in ordine alla circostanza che un tema fondamentale da affrontare sia quello relativo alle modalità tramite cui sarà possibile gestire il fenomeno pur nella consapevolezza che – posto che il nuovo Codice dei contratti pubblici è entrato in vigore in tempi relativamente recenti e deve, pertanto, ancora ultimare la fase di sperimentazione – sarà solo l'applicazione pratica in concreto di detti strumenti e il contenzioso che ne scaturirà a consentire una analisi empirica *ex post* delle problematiche che gradualmente il giurista dovrà affrontare[2].

1. Caringella–Carbone–Rovelli 2024.
2. Barberio 2023-a.

Il brocardo *ubi societas, ibi ius*[3], dunque, nel rievocare il pensiero di Santi Romano, si colora di nuove ed inattese suggestioni riconoscendo appieno un ruolo anche alla comunità che vive e alimenta una realtà caratterizzata dall'immaterialità.

Non è chiaro al momento se le pubbliche amministrazioni e, nella specie, le stazioni appaltanti saranno in grado di cogliere pienamente la portata innovativa del citato d.lgs. n. 36/2023 e dotarsi degli strumenti adeguati per affrontare compiutamente le sfide che in prospettiva sono state loro poste, né è chiaro se la velocità con cui i cambiamenti tecnologici si stanno imponendo troverebbe ancora l'approvazione di Filippo Tommaso Marinetti che nel *Manifesto del Futurismo* volle riconoscere proprio alla velocità la definizione di "bellezza nuova".

È, tuttavia, pur vero che allo stato bisogna capire quale tipologia di intelligenza artificiale possa essere di supporto nel rispetto della normativa europea e nazionale in rilievo ed effettuare un'analisi degli esempi virtuosi inaugurati da alcuni soggetti pubblici, nonché della previsione di clausole tipo inserite nei contratti perfezionati con i fornitori dei predetti meccanismi di automazione.

Tale ricerca va, ad ogni buon conto, condotta avendo costantemente cura dell'indefettibilità del ruolo dell'agente umano che non deve mai assolutamente perdere i suoi valori di riferimento.

2. Esercizio delle pubbliche funzioni e automazione dei processi

È indubbio che le scelte di politica legislativa riguardanti il ricorso a strumenti di automazione implichino una valutazione preliminare in ordine all'opportunità di implementare tali strumenti e contestualmente richiamino delle considerazioni di natura etica.

Per vero, tuttavia, se le sensibilità proprie di ciascun ordinamento giuridico si sono caratterizzate per un approccio diversificato e l'adesione ad un'impostazione originale a seconda della cultura di riferimento, è altresì pacifico che – al pari degli operatori privati[4] – anche il potere pubblico, seppure con le peculiarità che lo contraddistingue, non possa non essere interessato dalla rivoluzione copernicana avviata con le nuove tecnologie[5].

A ben vedere, se inizialmente dottrina e giurisprudenza amministrativa[6] avevano mostrato un forte scetticismo in ordine all'utilizzo di sistemi fondati sull'intelligenza artificiale e sugli algoritmi al fine di pervenire a processi decisionali automatizzati, in un secondo momento hanno ritenuto ammissibile il ricorso a tali modelli anche con riguardo ad attività amministrative a contenuto discrezionale ove siano rispettati taluni principi fondamentali[7] – che verranno analizzati in dettaglio nel prosieguo del presente lavoro – quali in particolare la trasparenza algoritmica, l'intellegibilità del dataset utilizzato, la non esclusività della decisione da parte del meccanismo di automazione e il divieto assoluto di discriminazione algoritmica secondo cui non bisogna alimentare diseguaglianze rispetto a determinati individui o categorie degli stessi.

Nello specifico il regolamento (UE) 2024/1689, nell'affermare detti principi, non ignora la necessità di doverne meglio perimetrare l'ambito di applicazione, essendo il legislatore europeo consapevole che la previsione di regole espresse con concetti giuridici indeterminati o formulazioni generiche – per acquisire una consistenza definita – richiedano una declinazione più puntuale all'interno di fattispecie concrete e di contesti specifici[8].

La scelta della tipologia di intelligenza artificiale e modalità di utilizzo, del resto, non sono irrilevanti rispetto ai riflessi che si riverberano, prioritariamente, con riguardo alla trasparenza dei processi decisionali[9].

Basti considerare che il ricorso ad un modello di algoritmo deterministico consente tendenzialmente la piena intellegibilità – almeno fino al momento dell'applicazione concreta – di ciascun

3. Mazzamuto 2020.
4. Tosi 2024.
5. Mattarella 2024.
6. Taddei Elmi–Marchiafava 2023.
7. Ciriello 2023.
8. Cassano–Tripodi 2024.
9. Ruffolo 2020.

presupposto logico che ha portato allo sviluppo del processo decisionale.

Di contro, nel caso in cui si operi tramite un modello basato sul c.d. machine learning la regola su cui si fonda una decisione viene sviluppata dal sistema senza che la correlazione con i dati sia comprensibile o nota, tantomeno al programmatore del software che ha creato l'algoritmo[10].

Ciò con l'ovvia conseguenza che il ragionamento algoritmico non può risultare intelleggibile *in toto*.

Per cui un problema di cui occorre necessariamente tener conto è che maggiore sarà il grado di accuratezza e di precisione della decisione adottata sulla scorta di un sistema di machine learning più complesso sarà fornirne una spiegazione, ovverosia una congrua motivazione in punto di fatto e di diritto.

Ciascuna pubblica amministrazione, pertanto, nell'esercizio delle proprie attività istituzionali, risulta investita del duplice onere di rendere intelleggibili le modalità di funzionamento algoritmico e contestualmente di dover fornire una motivazione adeguata con riguardo agli esiti raggiungi nel processo decisionale[11].

A ben vedere, tuttavia, il rapporto tra la strumentalità dell'automazione rispetto alla decisione – che poi confluirà in un provvedimento amministrativo – e la centralità dell'apporto umano rendono evidente che si tratta di problematiche ancora poco percettibili in tutte le loro implicazioni e che emergeranno gradualmente in concreto nella pratica, imponendo, in caso di contenzioso, un sindacato del giudice amministrativo che potrà estendersi fino alla verifica della conformità dei dati utilizzati nel modello rispetto agli esiti emersi[12].

Ciò significa che un punto di osservazione privilegiato può essere quello che si incentra sulla gestione operativa di tali sistemi e addirittura sulla fase esecutiva del contratto.

Tanto premesso, nell'ambito delle attività in cui si esplicano i pubblici poteri, il tema della contrattualistica pubblica e dei suoi rapporti con le tecnologie abilitanti 4.0 assume – come già precisato – sicuramente un ruolo centrale e costituisce un'occasione di sperimentazione sia alla luce del modello costruito dal d.lgs. n. 36/2023 sia sulla scorta della circostanza che i contratti pubblici, essendo segnati dalla rilevanza dell'interesse pubblico anche nella fase esecutiva,[13] richiedono, a maggior ragione, una particolare attenzione con riguardo all'addestramento iniziale dell'algoritmo.

A tal proposito è opportuno evocare quella dottrina[14] che ha evidenziato come gli appalti pubblici consentano il soddisfacimento di interessi ultronei rispetto a quelli direttamente collegabili all'acquisto di un bene, giacché coinvolgono la collettività, la tutela dei diritti sociali e temi come l'innovazione e la sostenibilità ambientale.

Per tale ragione è necessario evitare che i contraenti privati si trovino in una posizione di supremazia tecnica e, quindi, esercitino una forza negoziale in grado di condizionare il contenuto stesso di un contratto.

Va, inoltre, considerato che l'incertezza creata dalla frammentarietà del sistema degli appalti pubblici e l'elaborazione di principi sottesi all'utilizzo dell'intelligenza artificiale che tuttora sono privi di una consistenza concreta palesano che solo l'applicazione pratica consentirà di costruire un modello ispirato a regole di garanzia e a scelte tecniche non ambigue[15].

Ciò fermo restando, è pur vero che difficilmente i soggetti pubblici – almeno nell'immediato o in tempi brevi – risulteranno in grado di perfezionare autonomamente degli strumenti informatici adeguati e verosimilmente dovranno più spesso rivolgersi al mercato optando per l'acquisto di sistemi di intelligenza artificiale messi a disposizione da privati; ciò con l'ovvia conseguenza che il soggetto pubblico si esporrà al rischio di dover rispondere dinanzi agli operatori economici coinvolti in una procedura di evidenza pubblica di un sistema sviluppato ed acquistato da terzi.

10. Taddei Elmi 2021.
11. Belisario–Cassano 2023.
12. Ciriello 2023.
13. Clarich 2023.
14. Gamero Casado 2023.
15. Caringella–Carbone–Rovelli 2024.

3. La digitalizzazione dei contratti pubblici

Il tema della digitalizzazione della pubblica amministrazione è senza dubbio uno dei più controversi per gli osservatori[16] più attenti all'impatto che negli ultimi tempi hanno avuto ed avranno le nuove tecnologie sul mondo del diritto.

Con il PNRR[17], del resto, le stesse istituzioni europee hanno riconosciuto grande centralità alla trasformazione digitale e agli effetti che quest'ultima può avere sull'azione amministrativa con riguardo alla piena realizzazione del principio di trasparenza, ai criteri di efficienza, efficacia ed economicità, nonché alla prevenzione e al contrasto dei fenomeni di *maladministration*[18].

È indubbio, d'altra parte, che l'utilizzo di dati in formato digitale e il contestuale ricorso a strumenti di tecnologia informatica nell'esercizio dell'attività amministrativa agevolino il miglior perseguimento dell'interesse pubblico cui ciascuna pubblica amministrazione deve orientare la propria azione e abbiano effetti positivi, sia diretti che indiretti, con riguardo ai tempi ed all'allocazione delle risorse umane ed economiche.

A ben vedere, pertanto, il pieno sviluppo della c.d. "amministrazione digitale" offre una nuova e più ampia prospettiva al principio di buon andamento della pubblica amministrazione sancito dall'art. 97 Cost. ove si consideri che favorisce una diversa organizzazione della macchina amministrativa e, con riguardo alla collettività, un'erogazione più funzionale dei servizi pubblici[19].

Il modello di riferimento è stato, in particolare, tracciato dal d.lgs n. 82/2005 (c.d. Codice dell'amministrazione digitale) con cui il legislatore cercò per la prima volta di fornire una risposta adeguata ai cambiamenti tecnologici in atto e di individuare le modalità tramite cui le pubbliche amministrazioni potessero attuare la trasformazione digitale, nonché dall'art. 3-*bis* della legge n. 241/1990, come modificato nel 2020, con cui si è evidenziato che ciascuna amministrazione – al fine di conseguire maggiore efficienza – deve agire sia nei rapporti interni con altre pubbliche amministrazioni che con soggetti esterni ricorrendo agli strumenti informatici e telematici[20].

Ciò fermo restando, il tema in discussione va affrontato alla luce della rilevanza che assume in relazione ai contratti pubblici.

In proposito basti considerare che già nell'abrogato Codice di cui al d.lgs. n. 50/2016 all'art. 44 si demandava al Ministero per la semplificazione e per la pubblica amministrazione di precisare – entro un anno dall'entrata in vigore del medesimo codice – le modalità tramite cui procedere alla digitalizzazione delle procedure di gara, mentre all'art. 58 si riconosceva alle stazioni appaltanti di ricorrere interamente a procedure gestite con sistemi informatici pur nel rispetto dei principi della parità di accesso e della concorrenza.

Una vera e propria digitalizzazione delle procedure, tuttavia, nella vigenza del vecchio Codice – pur contemplando l'interconnessione e l'interoperabilità dei dati in possesso delle pubbliche amministrazione – non è mai avvenuta in considerazione della circostanza che il decreto attuativo è intervenuto con grave ritardo solo con il d.m. n. 148 del 12 agosto 2021 e che la disciplina appariva, in ogni caso, incompleta[21].

È, pertanto, proprio alla luce dell'introduzione del nuovo Codice dei contratti pubblici ai sensi del d.lgs. n. 36/2023 che il tema in commento ha assunto una nuova prospettiva per l'ambizione di rendere interamente digitale ed interoperabile ogni attività riguardante le procedure di evidenza pubblica nella loro interezza, ovvero per tutto il ciclo di vita dei contratti dalla loro fase embrionale a quella esecutiva.

Ci si riferisce, in particolare, al procedimento che viene avviato generando i c.d. c.u.p (codice unico di progetto) ed il c.i.g. (codice identificativo di gara), di cui è ben nota la funzione precipua di prevenire le frodi e l'elusione del divieto di doppio finanziamento europeo, e si sviluppa nelle attività incentrate sulla conclusione ed esecuzione del

16. Mattarella 2024.
17. Si fa riferimento alla Missione 1 incentrata su "Digitalizzazione, innovazione, competitività, cultura e turismo".
18. Merenda 2023.
19. Carloni 2024.
20. Clarich 2023.
21. Caringella–Carbone–Rovelli 2024.

rapporto negoziale con l'operatore economico che risulta aggiudicatario e con cui viene perfezionato il contratto[22].

Più nel dettaglio non si può non considerare che il Capo II della Parte I del Codice è incentrato proprio sulla digitalizzazione.

Un'attenta analisi al riguardo permette, in particolare, di cogliere immediatamente la diversa sensibilità con cui il legislatore del 2023 ha voluto valorizzare l'aspetto tecnologico proprio sulla scorta delle spinte provenienti dal PNRR che, tra i propri obiettivi[23], ha previsto di realizzare un sistema nazionale di *e-Procurement* al fine di digitalizzare *in toto* le procedure di acquisto, a cominciare dall'abilitazione digitale degli operatori economici, dall'utilizzo del machine learning per lo studio delle tendenze, nonché di chatbot evoluti di supporto e di *status chain*.

La decisa volontà legislativa di attribuire un ruolo centrale alla digitalizzazione, d'altra parte, è desumibile proprio dalla previsione dei principi che la caratterizzano (principi di neutralità tecnologica, di trasparenza, nonché di protezione dei dati personali e di sicurezza informatica) e di una disciplina organica che valorizza il ricorso alle piattaforme, il regime di pubblicità legale, il fascicolo virtuale dell'operatore economico e la previsione di una banca dati nazionale dei contratti pubblici di cui risulta titolare l'Anac[24].

Il fine ultimo è quello di costruire un sistema interconnesso e interoperabile che, grazie alla creazione di documenti nativo-digitali e procedure interamente digitalizzate, sia in grado di acquisire facilmente dati ed informazioni, nonché contestualmente di svolgere facilmente e rapidamente attività defatiganti che richiedono l'analisi di plurimi documenti, quale può essere la verifica dei requisiti di partecipazione di uno specifico operatore economico alle procedure di gara o la valutazione dell'offerta tecnica nella scelta del contraente.

4. Procedure automatizzate e principi di riferimento

Se la digitalizzazione nelle previsione del legislatore è finalizzata ad incidere sull'intero ciclo di vita dei contratti pubblici, è pur vero che una delle previsioni con maggiore portata innovativa è contenuta all'art. 30 del Codice, laddove si riconosce espressamente piena legittimazione a strumenti che consentano di automatizzare le attività mediante soluzioni tecnologiche, tra cui – in particolare – l'intelligenza artificiale e le tecnologie di registri distribuiti[25].

L'adeguata allocazione delle risorse al fine di un miglior perseguimento dell'interesse pubblico esige che vengano adottati dei sistemi tecnologici per contrastare le inefficienze ed i fenomeni di *maladministration*, ma anche e soprattutto per rispondere alle esigenze di accountability sempre più avvertite negli ordinamenti moderni[26].

Ne deriva conseguentemente che – per esigenze di funzionalità – il legislatore suggerisce il ricorso agli strumenti di automazione come regola generale che può essere derogata solo in determinati e specifici casi concreti.

Alla luce di quanto suesposto appare, dunque, ineludibile chiedersi in presenza di quali presupposti sia possibile per le stazioni appaltanti avviare e concludere le procedure di affidamento mediante sistemi di automazione e quale sia il perimetro all'interno dei quali detti sistemi possano incidere nella valutazione delle offerte.

Il Codice dei contratti pubblici contiene, del resto, la prima disciplina nazionale che ha individuato i principi da avere come riferimento in caso di ricorso a procedimenti amministrativi automatizzati ed a tecnologie avanzate.

Nella relazione di accompagnamento allo schema del d.lgs. 36/2023 il legislatore, conscio che nelle procedure di gara si utilizzino già degli algoritmi per il confronto automatico di taluni parametri – perfettamente conoscibili – propri delle offerte economiche, dichiara espressamente che l'art. 30

22. Orientamenti per la pianificazione dell'anticorruzione e della trasparenza approvati dall'Anac il 2 febbraio 2022.
23. La riforma M1C1-75 ha previsto la realizzazione del Sistema Nazionale di *e-Procurement* con riguardo particolare alla digitalizzazione completa delle procedure di acquisto fino all'esecuzione del contratto (*Smart Procurement)*.
24. Caringella–Carbone–Rovelli 2024.
25. Barberio 2023.
26. Rombi 2014.

aspira a disciplinare "il futuro prossimo" e che l'obiettivo immediato è quello di avere a disposizione degli algoritmi di apprendimento da utilizzare per le procedure di evidenza pubblica più complesse[27].

Inoltre, sebbene si tratti di una disposizione che caratterizza l'ambito della contrattualistica pubblica, è pur vero che con *vis espansiva* possa essere considerata in grado di costituire un riferimento per l'utilizzo delle nuove tecnologie con riguardo all'attività amministrativa nel suo complesso.

Tanto più ove si consideri che la modifica dell'art. 3-*bis* della l. n. 241/1990 già ha ribadito che l'uso dello strumento informatico debba rappresentare la regola per ciascuna amministrazione pubblica e che, a ben vedere, detti principi sembrerebbero rimarcare quanto altresì previsto dal Regolamento (UE) 1689/2024 (c.d. *AI Act*).

Quest'ultimo, peraltro, sembrerebbe a sua volta aver fatto propri i limiti e principi fondanti della normativa sul trattamento dei dati personali e lascia all'interprete il compito di perimetrarne l'ambito di applicazione.

Ad ogni buon conto qualsiasi dibattito sull'intelligenza artificiale non può prescindere dal costante riferimento a tali principi, considerato che la loro definizione dipende altresì dalle specificità del sistema che si intende costruire, nonché dalle modalità con cui viene utilizzato e dal contesto in cui opera.

Fermo ed impregiudicato che debba essere garantita la "riserva di umanità", soprattutto con riguardo alle attività a contenuto discrezionale, e che, in ogni caso, alla tecnologia – come avevano già diffusamente e ripetutamente osservato autorevole dottrina[28] e la giurisprudenza amministrativa[29] più sensibile al tema – debba essere riconosciuto un ruolo servente e strumentale, si tratta preliminarmente di demandare alle macchine attività di supporto o comunque ripetitive.

4.1. La comprensibilità e la conoscibilità

Il legislatore, consapevole della necessità di assicurare il bilanciamento degli interessi sottesi contrapposti, ha – in primo luogo – previsto che il contributo di sistemi che automatizzino i processi decisionali debba garantire la conoscibilità o comunque la comprensibilità di detti processi al fine di consentire a ciascun operatore economico di avere piena contezza dei processi automatizzati eventualmente utilizzati con riguardo specifico ad un suo interesse giuridicamente tutelato e a ricevere tutte le informazioni significative sulla logica che è stata adoperata.

Centrale, dunque, diviene la trasparenza con riguardo sia alla metodologia prescelta per l'assunzione di una determinata decisione con processi automatizzati, sia con riguardo al diritto di un singolo (i.e., l'operatore economico) di venire a conoscenza dell'esistenza di detti processi qualora lo riguardino[30].

Quest'ultimo aspetto, peraltro, va coniugato con l'ulteriore obbligo, previsto a carico delle pubbliche amministrazioni, di pubblicare sul proprio portale l'elenco delle soluzioni tecnologiche utilizzate nel corso dello svolgimento delle proprie attività istituzionali per disincentivare un uso non in linea con la disciplina applicabile da parte dei soggetti privati e pubblici e contestualmente consentire una conoscenza diffusa e, quindi, di esercitare una forma di controllo da parte della collettività .

Si afferma, in tal modo, un'accezione rafforzata del principio della trasparenza, laddove emerge che il legislatore – come ha brillantemente sostenuto il Consiglio di Stato nella sentenza n. 2270/2019 – vuole garantire che vi sia "una piena conoscibilità della regola espressa in un linguaggio differente da quello giuridico".

Ne consegue, pertanto, che – per garantire la conoscibilità e la comprensibilità del sistema utilizzato – sussiste in capo alla pubblica amministrazione coinvolta un gravoso obbligo di motivazione con la duplice finalità di riconoscere pienamente *ex* artt. 24 e 113 Cost. l'esercizio del diritto di difesa da parte di chi subisca un pregiudizio dal provvedimento amministrativo impugnato e

27. "La digitalizzazione dei ciclo di vita dei contratti", parte II della Relazione di accompagnamento al nuovo codice dei contratti pubblici.

28. Gallone 2023.

29. Consiglio di Stato, sentenze n. 2270/2019 e n. 88/2020.

30. Sapienza 2024.

contestualmente di consentire un'estensione del sindacato del giudice amministrativo[31].

Pur essendo quest'ultimo argomento estraneo al presente lavoro, è tuttavia di interesse dedicare una breve riflessione ai vizi di legittimità che potrebbero rilevare per provvedimenti amministrativi adottati sulla scorta di processi decisionali automatizzati che, oltreché per violazione di legge e incompetenza, potrebbero essere impugnati per eccesso di potere grazie ad una nuova declinazione delle sue figure sintomatiche.

Si pensi, in particolare, al travisamento o alla erronea valutazione dei fatti considerati dai sistemi algoritmici, allo sviamento di potere, all'illogicità o alla contraddittorietà dell'atto derivante dall'illogicità o contraddittorietà del *dataset* utilizzato, alla contraddittorietà tra più atti sulla scorta di un errore di calcolo, alla disparità di trattamento o all'ingiustizia manifesta in virtù di discriminazione algoritmica, ai vizi della volontà che interessano il processo decisionale automatizzato o alla mancanza di idonei parametri di riferimento[32].

4.2. La riserva di umanità

Viene, in secondo luogo, sancito il principio della non esclusività della decisione algoritmica prevedendo che nel processo decisionale vi sia sempre un contributo umano investito di una specifica attività di controllo, validazione, ovverosia della possibilità di smentita della decisione assunta con modalità automatizzate. Tale principio, sintetizzato nell'elegante espressione "riserva di umanità", ha una duplice valenza: da una parte impone il contributo umano nell'adozione di una scelta, dall'altra espone il medesimo agente ad una forma di responsabilità rafforzata, onerandolo della necessità di acquisire a sua volta una piena conoscenza del funzionamento degli algoritmi utilizzati[33].

Si richiede, pertanto, che i sistemi utilizzati siano sottoposti alla sorveglianza umana imponendo che i soggetti preposti siano adeguatamente formati e con competenze tali da garantire un'efficace supervisione dei sistemi di intelligenza artificiale utilizzati, un'attività di prevenzione con riguardo alla cibersicurezza, nonché di monitoraggio per valutare il sistema in termini di adeguatezza ed efficacia, oltreché per individuare i correttivi richiesti per procedere ad un aggiornamento periodico.

Tale gravoso onere, che per taluni osservatori – in virtù dei profili di responsabilità che ne derivano – potrebbe semplicemente determinare la fuga delle stazioni appaltanti dal ricorso alle procedure automatizzate, tiene conto della circostanza che i pericoli maggiori scaturenti dal ricorso all'intelligenza artificiale non derivano dalla sua produzione e messa in commercio, ma dal suo utilizzo.

Si tratta, ad ogni buon conto, di un presidio imprescindibile affinché l'intelligenza artificiale rimanga strumentale[34] e al servizio di una pubblica amministrazione più efficiente e contestualmente consenta a detti meccanismi di riscuotere una forma di legittimazione sociale grazie all'aspettativa che la decisione automatizzata sia in ogni caso sottoposta a revisione da parte di un soggetto umano. La scelta operata dalla macchina, in tal modo, non può più considerarsi autonoma (*recte*: automatizzata), ma va più correttamente interpretata come assistita, ovverosia si tratta in ogni caso di una scelta imputabile ad un essere umano con il supporto di un sistema basato sull'intelligenza artificiale[35].

Tale lettura permette, dunque, di smentire che si stia assistendo alla nascita di un nuovo *genus* di provvedimento amministrativo per ribadire che, in ogni caso, si è in presenza di un provvedimento amministrativo tradizionale con gli adattamenti dovuti in virtù del ricorso ad una macchina di intelligenza artificiale che consente di accrescere le conoscenze dell'amministrazione e allo stesso tempo di acquisire uno spettro di dati maggiori anche per l'adozione di scelte discrezionali[36].

I vantaggi, dunque, sono *ictu oculi* molteplici. Si pensi, in particolare, all'attività di certificazione e verifica delle dichiarazioni dei cittadini acquisite sulla scorta dei quali adottare un provvedimento:

31. Mattarella 2024.
32. Caringella–Carbone–Rovelli 2024.
33. Gallone 2023.
34. Lalli 2023.
35. Simoncini 2019.
36. Si vedano al riguardo le sentenze del TAR Puglia n. 552/2022 e del TAR Campania n. 7003/2022.

l'automazione del processo consente di ridurre la possibilità di errori con risparmio di risorse.

Se ne trae, pertanto, un giovamento in termini di efficienza e trasparenza diminuendo le ipotesi di disparità, le contraddizioni logiche connotate all'esercizio di un potere discrezionale e la diminuzione di incertezze con la conseguenza di prevenire errori e pregiudizi umani. Ciò, in ogni caso, richiede che in ciascun assetto organizzativo sia ripensata l'assegnazione delle risorse umane potendosi ragionare sia sull'aumento che sulla diminuzione delle stesse[37].

Ciò fermo restando, è pur vero che quello della riserva di umanità risulterebbe essere un principio derogabile, per cui in astratto sarebbe ben possibile prestare il consenso allo svolgimento di attività esclusivamente automatizzate in assenza di qualsiasi forma di supervisione; ovverosia di meccanismi di controllo, di validazione ovvero di smentita.

È un argomento che si ricava a contrario dal c.d. GDPR, il Regolamento (UE) 16/679 sulla protezione dei dati – richiamato espressamente dal più recente Regolamento sull'intelligenza artificiale –, il cui art. 22 riconosce la possibilità di prestare consenso per rinunciare al "diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano"[38]. Per tale consenso, peraltro, sebbene debba essere esplicito, non è richiesta la forma scritta *ad substantiam*, ma solo *ad probationem*.

Nemmeno in siffatta ipotesi, tuttavia, si assiste ad una disumanizzazione del procedimento divenuto interamente automatizzato, poiché ciò non può mai comportare una deresponsabilizzazione assoluta del soggetto umano. È, del resto, il sistema costituzionale nel suo complesso ad essere costruito sulla responsabilità (personale) dell'uomo[39].

4.3. Il divieto di discriminazione algoritmica

Il titolare della procedura deve in ogni caso garantire la predisposizione di misure tecniche e organizzative adeguate finalizzate a scongiurare la denegata ipotesi che taluni errori sistematici e ripetibili finiscano per alterare l'elaborazione dei risultati. Il fenomeno, riconducibile alla definizione di discriminazione algoritmica, impone di utilizzare *dataset* ampi e completi al fine che non si creino dei pregiudizi – propri anche dell'essere umano – nei confronti di individui specifici o appartenenti a determinati gruppi sociali.

È, pertanto, indispensabile predisporre misure efficaci per rettificare quei fattori che possano alimentare effetti discriminatori e, dunque, pregiudizievoli nei confronti di persone fisiche per via del sesso, della nazionalità, dell'etnia, delle convinzioni religiose, delle opinioni politiche e dell'appartenenza ad una determinata organizzazione sindacale, ovvero sulla scorta dell'acquisizione di dati sensibili (si pensi, in particolare, allo stato di salute di taluni soggetti che potrebbe esprimere una valutazione con riguardo alla prestazione lavorativa).

Solo l'individuazione di *dataset* adeguati sia sotto il profilo qualitativo che quantitativo possono consentire di costruire un modello che non conduca a risultati parziali e che non sia errato o eccessivamente limitato[40].

La distorsione, del resto, può addirittura essere intrinseca al dataset utilizzato. Basti pensare a dati storici cui si fa ricorso che gradualmente possono moltiplicare in maniera esponenziale le discriminazioni esistenti.

Il tema, che importa problemi di grande complessità, assume rilevanza soprattutto con riguardo a sistemi di intelligenza artificiale ad alto rischio e richiede di prestare particolare attenzione alle potenziali distorsioni in grado di ingenerare pregiudizi per i diritti fondamentali[41] delle persone imponendo – come meglio si vedrà nel paragrafo dedicato alla tipologia di intelligenza artificiale che si ritiene più conferente alle procedure di gara – di attuare un modello di governance finalizzato all'attenuazione delle occasioni di potenziale distorsione.

37. De Minico 2022.
38. Pizzetti 2018.
39. Romano 2018.
40. Falletti 2022.
41. Avitabile 2017.

5. L'accesso al codice sorgente come espressione del diritto alla conoscenza e la previsione di clausole negoziali ai fini di un tempestivo intervento correttivo

Il citato art. 30 del Codice dei contratti pubblici, nel riconoscere alle stazioni appaltanti ed agli enti concedenti di ricorrere a soluzioni di automazione nell'espletamento delle loro attività istituzionali, contiene al secondo comma due indicazioni di assoluto rilievo: a) l'obbligo a carico di tali soggetti di garantire la disponibilità al codice sorgente del software utilizzato, alla documentazione di supporto e ad ogni altro ulteriore elemento ove sia ritenuto utile per comprenderne le logiche di funzionamento; b) l'inserimento di clausole, anche con riguardo agli atti di indizione della gara, finalizzate a consentire un intervento tempestivo per ovviare alla presenza di errori o effetti non voluti determinati dall'automazione mediante prestazioni di assistenza e di manutenzione.

Con la previsione di cui *sub* a), che introduce al più complesso tema relativo alla circostanza che la scelta del meccanismo di intelligenza artificiale da utilizzare non è mai neutrale, il legislatore impone al contraente pubblico di individuare entro quale perimetro potrà essere garantita la conoscenza e secondo quali modalità, nel contemperamento degli interessi contrapposti, si dovranno comprimere i diritti di proprietà intellettuale eventualmente coinvolti[42]. È del tutto evidente, dunque, che i problemi in rilievo risultano essere molteplici, soprattutto ove si consideri sembrerebbe necessario, tramite una valutazione da effettuarsi caso per caso, procedere ad una distinzione sulla scorta del tipo di algoritmo utilizzato, ovverosia sulla struttura del modello ed i dati immessi ai fini dell'addestramento.

Invero, nel caso in cui si sia in presenza di un algoritmo a struttura condizionale, almeno tendenzialmente, dovrebbe essere infatti possibile verificare e controllare le scelte e ricostruire i processi decisionali con le logiche ad esso sottese. Di contro, nel caso in cui sia stato utilizzato un sistema di machine learning, l'iter logico che ha consentito di pervenire ad una determinata decisione non può essere ricostruito a ritroso e, dunque, né controllato e verificato[43].

Emerge, dunque, la necessità di assicurare una forma di trasparenza *ex ante* anche sul tipo di procedura utilizzata che, al netto degli obblighi di pubblicazione già specificati, evoca altresì a carico delle stazioni appaltanti la necessità di assicurare la tracciabilità e trasparenza delle attività svolte in ossequio a quanto statuito dal sesto comma dell'art. 19 del d.lgs. n. 36/2023.

Bisogna, a ben vedere, capire se l'ostensione debba essere garantita sotto il profilo meramente formale, ovverosia se sia necessario altresì fornire un supporto all'interessato per decifrare il contenuto di quanto viene trasmesso e fare in tal modo comprendere conoscenze caratterizzate da elevato livello tecnico.

Una riflessione sul punto, peraltro, può condurre a ritenere preferibile, in luogo dell'acquisizione del codice sorgente, una conoscenza sui dati di *training* inseriti onde verificare e controllare se l'algoritmo sia stato creato con dati indicati per la fattispecie che in concreto viene in rilievo e quali dati abbiano maggiore peso nell'elaborazione di una determinata risultanza[44].

Occorre, inoltre, porre il rilievo che la possibile acquisizione della disponibilità del codice sorgente del software utilizzato non può di certo comportare una ostensione indiscriminata, laddove si consideri che l'accesso del privato interessato viene garantito ove esso risulti indispensabile per la tutela in giudizio di interessi giuridicamente rilevanti[45].

Sembrerebbe, pertanto, emergere una scissione tra il principio di trasparenza algoritmica – che costituisce un riferimento costante che trova piena realizzazione anche mediante gli obblighi di pubblicazione nella "sezione amministrazione trasparente" – e l'accesso al codice sorgente in cui le esigenze conoscitive in ordine alle logiche sottese al processo decisionale automatizzato rendono necessario un bilanciamento tra gli interessi contrapposti, in particolare tra le garanzie di difesa e i diritti di proprietà intellettuale, diritti che

42. Peluso 2023.

43. Amato Mangiameli 2022.

44. Cerrina Feroni–Fontana–Raffiotta 2022.

45. Orofino 2022.

assumono una fondamentale rilevanza nel contesto dello sviluppo di modelli innovati per la pubblica amministrazione[46].

Conseguentemente, mentre ciascun operatore economico coinvolto nella procedura di gara potrà conoscere dell'esistenza di processi decisionali fondati su sistemi di automazione e acquisire informazioni significative sulle logiche sottese, non è chiaro, invece, entro quali limiti sarà possibile accedere al codice sorgente, né con quali modalità potrà esercitarsi tale diritto in presenza di percorsi motivazionali che non sono ricostruibili *ex post*.

Con riguardo, invece, all'inserimento, già negli atti di indizione delle gare, di clausole contenenti prestazioni di assistenza e di manutenzione per scongiurare la presenza di errori o per porvi tempestivamente rimedio, va evidenziato che si tratta di una previsione con cui il legislatore, nel considerare insufficiente un giudizio – cristallizzato al momento dell'acquisto – sulla valenza del meccanismo di intelligenza artificiale utilizzato, richiede di individuare dei presidi – anche tecnici – per intervenire sulle modalità concrete di utilizzazione dell'algoritmo; con ciò invitando il soggetto pubblico ad assicurare una supervisione costante sul livello qualitativo (oltreché quantitativo) del sistema utilizzato per scongiurare il verificarsi di effetti pregiudizievoli.

A ben vedere, si riafferma sul piano esecutivo il principio secondo cui la stazione appaltante o l'ente concedente che vogliano servirsi di sistemi che consentano di utilizzare la decisione algoritmica debbano, in ogni caso, adottare quelle misure tecniche e organizzative per attuare un effettivo controllo, minimizzare i rischi e scongiurare che i fattori che determinano l'inesattezza dei dati non siano tempestivamente rettificati.

6. Intelligenza artificiale e contratti pubblici: ambito applicativo e presupposti

Un tema di sicuro rilievo e dal quale scaturirà un ampio dibattito non appena le stazioni appaltanti e gli enti concedenti vorranno dare pienamente applicazione al disposto di cui all'art. 30 d.lgs. n. 36/2023 è quello relativo al perimetro applicativo dell'intelligenza artificiale con riferimento ai contratti pubblici.

Prima di entrare in *medias res* si ritiene, tuttavia, fondamentale fornire una precisazione in ordine alla distinzione tra algoritmo e sistemi di intelligenza artificiale.

Il Consiglio di Stato con l'arresto n. 7891 del 2021 ha chiarito che tra algoritmo di trattamento e sistemi di intelligenza artificiale vi è una differenza di natura ontologica che ha rilievo con riguardo agli effetti materiali prodotti e al regime applicabile.

Nello specifico alla nozione di algoritmo corrisponde una sequenza finita di istruzioni e dal significato univoco che possono essere eseguite in modo meccanico al fine di consentire il raggiungimento di un determinato risultato. Gli algoritmi, del resto, sono fondati su uno schema tipico che contempla tre momenti: input, elaborazione e risposta. Tale nozione, ove sia inserita all'interno di piattaforme tecnologiche, evoca sistemi di azione e di controllo che consentono di diminuire l'intervento dell'agente umano.

Trattandosi quindi di dare esecuzione ad istruzioni definite e non ambigue in presenza di specifici presupposti, la sequenza algoritmica vincola il sistema informatico all'esecuzione di operazioni già prestabilite.

Si è, invece, in presenza di un sistema di intelligenza artificiale allorché l'algoritmo preveda dei meccanismi di machine learning in grado di elaborare un risultato non già sulla scorta di regole e parametri predefiniti, ma in virtù di nuovi criteri di inferenza tra i dati. Si realizza così un processo di apprendimento automatico che consente al sistema di rielaborare i dati progressivamente acquisiti e di sviluppare le decisioni in autonomia[47].

Ne consegue, pertanto, che con detti sistemi non si assiste alla mera esecuzione meccanica di determinate istruzioni sulla scorta di una sequenza algoritmica, ma si afferma una capacità di autoapprendimento in grado di consentire un adeguamento costante.

Detta distinzione, riportata sinteticamente solo ai fini del presente lavoro, è di supporto al fine di perimetrare immediatamente l'ambito entro cui i sistemi di intelligenza artificiale possono avere un ruolo con riferimento ai contratti

46. Farina 2023.

47. Bellini–Guidi 2022.

pubblici e individuare – sulla scorta del citato art. 30 – la tipologia di intelligenza che risulta più aderente alle specifiche esigenze avvertite dalle stazioni appaltanti.

Orbene, un ambito in cui gli strumenti di automazione possono assumere un ruolo centrale è sicuramente quello relativo alla fase istruttoria delle procedure di evidenza pubblica con particolare riguardo al momento della valutazione delle offerte.

In merito va subito evidenziato che, giacché per la comparazione delle offerte economiche si utilizzano già formule alfanumeriche per il cui sviluppo l'intelligenza artificiale non è di supporto, è chiaro che un ampio spazio possa riconoscersi precipuamente con riguardo alla valutazione delle offerte tecniche.

Invece, per quanto si tratti di un dibattito di grande fascino, non sembrerebbe ipotizzabile, almeno nel breve termine e indipendentemente dai meccanismi illustrati nei paragrafi precedenti, poter procedere ad effettuare scelte discrezionali tramite il ricorso a veri e propri provvedimenti automatizzati.

Volendo, pertanto, soffermarsi sulla valutazione delle offerte tecniche, i modelli di intelligenza artificiale più adeguati alle specifiche finalità perseguite sembrerebbero essere quelli basati sui *Large Language Models* (LLMs).

Si tratta, più in particolare, di modelli caratterizzati dalla capacità di elaborare un riscontro pressoché immediato e apprezzati per la qualità degli esiti forniti grazie ad adeguati input sorgenti (c.d. prompt) in grado di generare una sequenza di dati e codici corrispondenti alle finalità perseguite[48].

Nell'ambito di tali modelli possiamo considerare Gopher, OPT4, LaMDA, GPT-3 e PaLM.

Tutto ciò premesso, il conseguimento di risultanze conferenti, efficaci e in ogni caso orientate allo scopo perseguito con riferimento agli appalti pubblici richiedono la sussistenza di due presupposti indefettibili.

Viene in primo luogo in rilievo il training, ovvero il sistema di addestramento orientato su una attività istruttoria predefinita.

Detto presupposto richiede che sia sviluppato un adeguato modello di apprendimento automatico (machine learning) o addirittura di apprendimento profondo tramite reti neurali (deep learning) in grado consentire lo sviluppo automatico di abilità e conoscenze; con ciò sviluppando anche una autonomia di azione rispetto ai controlli umani che potrebbe alimentare plurime problematiche. Tanto più ove si consideri che il grado di autonomia variabile, proprio di tali sistemi, potrebbe essere tendenzialmente assoluto.

È pur vero, tuttavia, che detta forma di autonomia trova la sua fonte nel contesto in cui detti sistemi operano e che quest'ultimi sono addestrati sulla scorta degli input forniti, per cui gli esiti che se ne ricavano risentono a livello qualitativo dell'ambiente che li plasma.

Ne consegue che – al fine di prevenire eventuali riscontri asseritamente discriminatori o comunque errati, limitati e parziali – non bisogna soffermarsi principalmente sulla tipologia di algoritmo adoperato, bensì sull'ambiente e sui dati che al momento dell'addestramento possano ritenersi sufficientemente adeguati in termini quantitativi e qualitativi.

Il secondo presupposto indefettibile evoca, invece, la predisposizione di un sistema di governance adeguato o, meglio, di presidi volti ad effettuare dei controlli e delle verifiche penetranti sia *ex ante* che *ex post*. Un presidio preventivo efficace consente, del resto, di favorire le condizioni ottimali per addestrare il sistema in un ambiente adeguato[49].

Nell specifico si ritiene che al soggetto responsabile della gestione del meccanismo di automazione spetti altresì pianificare l'organizzazione di strutture *ad hoc* con cui attuare gli obblighi di sorveglianza umana, nonché gestire le procedure di reclamo e di ricorso.

La prospettiva, in particolare, è duplice: a) in un'ottica preventiva è necessario predisporre un piano di valutazione dettagliato che, nel raccogliere le informazioni necessarie e nel descrivere l'impatto che sotto il profilo qualitativo e quantitativo può avere il sistema di intelligenza artificiale, individui altresì le misure e gli strumenti per mitigare i rischi con particolare riferimento ai diritti fondamentali astrattamente pregiudicati dal concreto uso del predetto sistema; b) in un'ottica di controllo

48. Pesucci 2022.

49. Caringella–Carbone–Rovelli 2024.

e verifica elaborare un presidio per il monitoraggio continuo volto a misurare l'adeguatezza e l'efficacia del sistema nel tendenziale rispetto dei principi esposti in precedenza.

La necessità di effettuare una valutazione d'impatto preliminare[50] sul sistema concretamente utilizzato in relazione al contesto in cui opera è un modello che sul piano europeo ha già trovato applicazione in altri settori sensibili. Si pensi al Regolamento 85/337/CEE in ordine alla valutazione d'impatto ambientale, all'art. 35 del Regolamento (UE) 2016/679 sulla valutazione d'impatto sulla protezione dei dati derivante dal ricorso alle nuove tecnologie, ma anche alle tecniche proprie della prevenzione e del contrasto alla corruzione.

Detta forma di precauzione richiede, tra l'altro, la predisposizione di misure rafforzate, in particolare allorché si ricorra a sistemi di intelligenza artificiale ad alto rischio con i quali aumentano le possibilità di assistere ad ipotesi di discriminazione algoritmica là dove non siano operati controlli, verifiche o smentite adeguati. Individuare dei rigorosi presidi di controllo consente, invero, di migliorare e vagliare l'efficacia del sistema, ma anche di legittimarne l'utilizzo, fermo restando che le sfide poste dalle tecnologie abilitanti 4.0 impongono di individuare soluzioni che vadano oltre i sistemi di controllo e di verifica di tipo tradizionale ricorrendo, se del caso, anche ad enti terzi certificatori che possano offrire servizi di conformità dei dati o effettuare una verifica sul sistema dei presidi e delle pratiche di addestramento, convalida e prova dei dati. Sotto quest'ultimo profilo assume specifico rilievo la pubblicazione della ISO/IEC 42001:2023 che – nella prospettiva del pieno recepimento dell'*AI Act* europeo e dell'*Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence* emanato dal governo USA il 30 ottobre 2023 – intende garantire il rispetto dei diritti fondamentali, della riservatezza e della sicurezza della generalità dei consociati favorendo la predisposizione di meccanismi e di presidi di controllo modellati in concreto sugli specifici sistemi algoritmici adottati e sulle esigenze dell'apparato che faccia richiesta della certificazione. L'idea è, in sintesi, quella di creare un Sistema di Gestione dell'Intelligenza Artificiale (AIMS, *Artificial Intelligence Management System*) che, oltre ai già previsti standard di interoperabilità introdotti dalla più recente disciplina europea, garantisca altresì il rispetto delle altre norme ISO già esistenti, valorizzando i processi di verifica e di controllo, nonché la sicurezza dei sistemi algoritmici basati sull'IA. Si tratta, a ben vedere, si fornire adeguate garanzie con riferimento ai meccanismi di automazione decisionale, al ricorso a metodologie non verificate di analisi con *dataset* basati sull'IA, nonché a processi di apprendimento che non sempre appaiono prevedibili.

Per tali ragioni, anche con riguardo alle specifiche tecniche *ex* art. 79 e all. II.5 del Codice dei contratti pubblici, è altresì auspicabile che il sistema, prima di essere utilizzato nelle procedure di gara, sia certificato in relazione al contesto in cui è avvenuto l'addestramento, all'adeguatezza ed alla rappresentatività dei dati.

Se da un punto di vista procedurale non è peregrino ipotizzare strutture *ad hoc* che contemplino dei meccanismi di *audit* o di verifica della performance nel corso del ciclo di vita del contratto con particolare riguardo all'esecuzione dello stesso, sotto il profilo sostanziale è però necessario valorizzare quei sistemi di intelligenza artificiale che siano caratterizzati da trasparenza e adeguata accuratezza, nonché da seri presidi idonei a depurarli dai potenziali fenomeni di discriminazione algoritmica.

È opportuno, più in particolare, che i *dataset* utilizzati siano di elevata qualità ai fini dell'addestramento e siano mirati al perseguimento della finalità indicata senza essere coinvolti in usi impropri. Il rischio, del resto, è precipuamente quello di alimentare delle distorsioni intrinseche utilizzando dati storici che possano generare discriminazioni[51].

In siffatta ipotesi le risultanze elaborate dai sistemi risentono di tali distorsioni intrinseche e finiscono progressivamente per amplificare quello che è un vizio genetico degli stessi.

Non è un caso, dunque, se i sistemi di intelligenza artificiale ad alto rischio sono stati oggetto di particolare attenzione da parte del Regolamento (UE) 2024/1689 che, nella prospettiva che sia predisposto un apparato in grado di controllare, validare o smentire le decisioni automatizzate,

50. Ruffolo 2021.

51. Musti 2024.

all'art. 14 impone forme di supervisione in modo proporzionale ai rischi connessi alla salute, alla sicurezza ed ai diritti fondamentali che possono venire in rilievo.

Il legislatore europeo, conseguentemente, sembra orientarsi in senso negativo in ordine all'ammissibilità dei sistemi di apprendimento profondo (deep learning), sistemi che si connotano per il loro essere privi di qualsiasi apporto o intervento umano.

Con riguardo, invece, alle attività ad alto rischio, *prima facie* e sulla scorta di una analisi che si sofferma sul mero dato normativo, il settore dei contratti pubblici non dovrebbe rientrare in detta categoria.

L'art. 6 del citato regolamento europeo, del resto, a conferma di quanto detto, tra le attività ad alto rischio non fa rientrare gli appalti pubblici. Una verifica sostanziale e in concreto sull'operato di una stazione appaltante, tuttavia, potrebbe condurre ad una considerazione del tutto inversa, soprattutto con riferimento ad attività valutative intrinseche su fatti o disposizioni normative che importino conseguenze inerenti la gestione ed il funzionamento delle infrastrutture digitali critiche, alla prestazione e servizi pubblici e privati essenziali. A titolo esemplificativo, si pensi alla fornitura di gas, energia elettrica ed acqua[52].

Nell'ambito dei contratti pubblici è – si ripete – imprescindibile consentire lo sviluppo pieno di un ambiente adeguato ed attivare un sistema di supervisione che favorisca la restituzione di output logici e corretti che, in caso contrario, conformemente al Regolamento (UE) 2024/1689, vengano smentiti in seguito a controlli e verifiche effettuati da sorveglianti umani con un "livello sufficiente di alfabetizzazione".

In sostanza, il sistema di governance dovrebbe consentire di individuare preventivamente i rischi e predisporre i meccanismi per limitare gli effetti pregiudizievoli e le conseguenze negative derivanti dal sistema di intelligenza artificiale.

Tale esigenza, del resto, è condivisa anche dal legislatore europeo nel citato Regolamento, sebbene quest'ultimo si sia soffermato sui rischi di discriminazione algoritmica e sulla violazione dei diritti individuali senza riconoscere la necessaria centralità ai rischi – derivanti dal malfunzionamento del sistema di intelligenza artificiale – correlati alla restituzione di dati erronei e/o parziali che non è più possibile controllare.

7. Le "clausole tipo" della Commissione europea nei rapporti tra soggetti pubblici e fornitori privati

Al fine di promuovere la diffusione di meccanismi di automazione caratterizzati, almeno in linea di principio, da affidabilità e trasparenza, la Commissione europea – già prima che fosse approvato il Regolamento (UE) 2024/1689 – ha ritenuto opportuno ipotizzare delle clausole negoziali standard per promuovere l'acquisto e l'utilizzo di detti meccanismi. Pur non essendo contenute in un documento ufficiale dell'Unione europea, a prescindere dal contenuto e dalla necessità di aggiornare le clausole in commento, esse costituiscono un virtuoso tentativo – almeno nelle intenzioni dei predisponenti – di fornire uno strumento utile ai fini della regolazione dell'acquisto dei sistemi di intelligenza artificiale da parte di operatori pubblici.

Al riguardo taluni osservatori hanno richiamato il valore normativo delle clausole d'uso in considerazione del ruolo che il soggetto pubblico riveste. In prospettiva, dunque, a seconda dei casi concretamente in rilievo, la disciplina dei provvedimenti di regolazione potrà essere recepita o mutuata in specifiche clausole fino a divenire vere e proprie prassi negoziali[53].

Le clausole ipotizzate dalla Commissione europea, in particolare, sono ascrivibili a due distinti modelli, definiti completi o leggeri a seconda che coinvolgano o meno sistemi di intelligenza artificiale ad alto rischio[54]. Conseguentemente l'inquadramento di un meccanismo di automazione tra i sistemi ad alto rischio comporta da parte del contraente pubblico una diversa modulazione del regolamento negoziale sulla scorta della necessità di adottare maggiore cautela.

Tanto premesso, prima di analizzarne i tratti salienti con riguardo ad alcune clausole tipo,

52. Cassano–Tripodi 2024.

53. Belisario–Cassano 2023.

54. Il gruppo denominato *Procurement for AI community* ha sviluppato due distinte proposte con riguardo alle clausole standard da inserire nei contratti pubblici.

va considerato che si tratta in genere di clausole caratterizzate da contenuti generici e indefiniti che non consentirebbero – in ogni caso – un effettivo supporto.

Di fatto dette clausole non si connotano né per il contenuto regolatorio compiuto, né per essere un supporto idoneo per rispondere alle esigenze e alle finalità di cui pure cercano di tener conto. Di contro sono gli operatori di mercato che si trovano in una posizione di supremazia tecnologica tale da poter esprimere un potere negoziale in grado di imporre clausole che potrebbero incidere sulla tutela dei diritti fondamentali pregiudicati dai processi decisionali.

Nello specifico si consideri che, in riferimento al modello ad alto rischio, si richiede di introdurre una clausola con cui il fornitore si obbliga a favorire la comprensione del contraente pubblico sul funzionamento del sistema di intelligenza artificiale, nonché a fornire ogni informazione che si renda utile con riferimento altresì alle specifiche tecniche e ad illustrare il ragionamento seguito dal sistema per pervenire ad una determinata decisione.

Ebbene, pur nella prospettiva di garantire il principio di trasparenza, nel documento della Commissione europea non ci si sofferma sui requisiti tecnici minimi richiesti, né vi è alcun accenno all'obbligo di rendere disponibili i codici sorgente, i dati utilizzati e la documentazione di supporto.

Altro tema è poi quello relativo alle clausole relative alla "riserva di umanità" che, tuttavia, importano considerazioni del tutto speculari a quelle testé esposte. Quest'ultima tipologia di clausole impone che il sistema di intelligenza artificiale – in misura progressivamente maggiore a seconda dei rischi che potrebbero emergere – sia progettato e sviluppato in modo da garantire sotto il profilo sostanziale un effettivo, pertinente ed adeguato controllo del preposto umano. La clausola in questione, così come congegnata, pur ponendo in luce un aspetto centrale, finisce per essere meramente pleonastica, ove si limita a richiamare un principio generale che informa l'utilizzo dell'intelligenza artificiale rinviando a definizioni dal contenuto indeterminato quale è quello di proporzionalità ed effettività.

Sarebbe, per tale motivo, auspicabile individuare dei requisiti tecnici e organizzativi minimi al fine di valorizzare in concreto sul piano negoziale il principio generale che vieta che le decisioni siano adottate esclusivamente mediante l'utilizzo di strumenti di automazione in assenza di un contributo umano.

È quest'ultima, del resto, una delle principali questioni che dovrà affrontare l'autorità amministrativa indipendente che, nell'esercizio del proprio potere regolatorio, dovrà individuare degli elementi di concretizzazione per facilitare lo sviluppo delle nuove tecnologie nel settore dei contratti pubblici.

8. Contratti pubblici e esperienze virtuose

Come si è già avuto modo di precisare, l'ambito in cui le nuove tecnologie possono esprimere le maggiori potenzialità con riferimento ai contratti pubblici è sicuramente legato alla fase istruttoria e alla valutazione delle offerte tecniche. Sebbene al momento gli sviluppi cui assisteremo di qui a breve risultano essere imprevedibili, è pur vero che è ben possibile analizzare le sperimentazioni già avviate da parte di taluni soggetti che direttamente o indirettamente, nell'espletamento delle loro attività istituzionali, sono coinvolti nei contratti pubblici. Risulta, pertanto, di grande interesse dar conto delle esperienze più virtuose che si sono registrate nell'utilizzo delle procedure automatizzate con riguardo al tema *de quo* anche al fine di vagliare l'adeguatezza dei presidi che sono stati individuati dal legislatore.

8.1. Il ruolo della centrale d'acquisto nazionale della pubblica amministrazione

Il Piano Nazionale di Ripresa e Resilienza (PNRR) tramite la riforma *Recovery Procurement Platform* e, in particolare, il target[55] M1C175 ha riguardato la digitalizzazione degli appalti pubblici, come si è avuto modo di illustrare. Ciò ha favorito l'interoperabilità tra la piattaforma di *e-Procurement* ed

55. L'attuazione del PNRR è scandita da tempistiche stringenti e prevede alcuni step intermedi distinguendo tra *milestone* (traguardi) e *target* (obiettivi). Con le prime si misurano i traguardi qualitativi (ad esempio le riforme legislative o l'operatività di un sistema informativa) mentre i secondi considerano gli obiettivi quantitativi misurati tramite indicatori ben specificati (l'aggiudicazione di una gara, l'acquisto di una fornitura, l'esecuzione di lavori).

i servizi centralizzati di Anac, l'individuazione di nuove modalità di autenticazione degli operatori economici e, in particolare, la creazione di un nuovo fascicolo virtuale dell'operatore economico che garantisce un accesso costante, la disponibilità del fascicolo di gara e l'espletamento dei controlli in ordine al possesso dei requisiti di partecipazione[56].

La digitalizzazione integrale delle procedure d'acquisto richiede che gli operatori economici ricevano una specifica abilitazione digitale, possano partecipare a sessione d'asta digitali e – per quanto d'interesse ai fini del presente lavoro – siano utilizzati sistemi di machine learning per il monitoraggio e l'analisi delle tendenze, nonché un'assistenza costante con chatbot e *status chain*.

Consip s.p.a., da centrale d'acquisto nazionale della pubblica amministrazione, è dunque tra i principali soggetti destinatari della riforma ed ha avuto modo, per tale ragione, di sviluppare iniziative che potrebbero fungere da modello per altre sperimentazioni[57].

Nello specifico si è intervenuti sul servizio di assistenza e di supporto (c.d. CRM, acronimo di *Customer Relationship Management*) con un meccanismo di chatbot evoluto che costituisce il canale di comunicazione utilizzato dai soggetti coinvolti nelle procedure di appalto pubblico ed è finalizzato a rendere questi ultimi autonomi nella risoluzione delle problematiche che possono di volta in volta emergere. Le funzionalità di cui dispone detto chatbot sono, peraltro, in grado di effettuare un'attività di analisi e monitoraggio delle interazioni occorse con gli utenti e, tramite una profilazione dei dati, di ottimizzare le iniziative di *customer care*[58].

Si è, in secondo luogo, ritenuto di adottare tecnologie avanzate di intelligenza artificiale ricorrendo ad un sistema (MePaWatch)[59] in grado di rielaborare le informazioni acquisite tramite le transazioni, avvenute nell'ultimo triennio, effettuate da soggetti pubblici e da operatori economici sul mercato elettronico della pubblica amministrazione[60]. Detta applicazione, grazie al machine learning ed agli indicatori comportamentali, è in grado di monitorare le condotte ritenute virtuose che periodicamente vengano in rilievo e di analizzare l'eventuale sussistenza di occorrenze che non siano in linea con il Codice dei contratti pubblici[61].

Nello specifico si può ritenere che si tratti di un modello previsionale che, grazie ai sistemi di intelligenza artificiale, è in grado di analizzare i dati storici relativi alle iniziative di acquisto e – sotto il profilo dinamico – i trend in atto, segnalando l'eventuale presenza di violazioni o situazioni lesive per i principi della concorrenza, del mercato e della trasparenza, nonché fenomeni corruttivi. Detta analisi permette, dunque, di adottare le dovute azioni correttive, laddove emergano comportamenti non previsti e fattori di rischio.

56. Si attua un'integrazione funzionale della piattaforma di *e-Procurement* con la Piattaforma Contratti Pubblici (PCP) di Anac in ossequio a quanto previsto dal d.lgs. n. 36/2023.
57. Vedi artt. 7, 12, 21, 29 del d.lgs. n. 36/2023. AgID ha predisposto le Regole tecniche per l'interoperabilità tra le piattaforme ed il relativo processo di certificazione completato il 26 settembre 2023. Consip ha ottenuto la certificazione prevista ed è stata iscritta nel registro gestito dall'Anac. Dal primo gennaio 2024 tutte le fasi del ciclo di vita dei contratti pubblici sono gestite in modalità digitale grazie all'integrazione dei servizi esposti sulla Piattaforma Digitale Nazionale Dati (PDND).
58. L'iniziativa è stata illustrata a ForumPA, evento tenutosi a Roma al palazzo dei Congressi dal 21 al 23 maggio 2024.
59. Orofino 2022.
60. Il sistema, che consente una analisi del MEPA (Mercato elettronico della pubblica amministrazione), è stato sviluppato a partire dalla fine del 2021. Il MEPA, introdotto con il d.p.r. n. 101/2002, permette alle amministrazioni pubbliche di ricorrere alle procedure telematiche per l'acquisto di beni e servizi sottosoglia. Si tratta di uno strumento che rende più trasparenti, semplici e rapidi i processi di acquisto garantendo al contempo la massima partecipazione degli operatori economici. Consip interviene sia in fase di predisposizione delle condizioni generali di forniture che per la definizione delle categorie merceologiche e l'abilitazione degli operatori economici.
61. Si rinvia all'accordo quadro sottoscritto il 2 agosto 2024 2024 da Consip con AgID – Agenzia per l'Italia Digitale.

Il machine learning, dunque, favorisce l'adozione di modelli predittivi innovativi e lo sviluppo di analisi quantitative che consentono, tramite una valutazione fondata su un calcolo statistico e sul criterio della probabilità, di attivare un alert in presenza di comportamenti non ritenuti conformi ai principi generali che regolano il mercato. Ciò dovrebbe determinare due conseguenze positive: da una parte, semplificherà le decisioni e la partecipazione delle pubbliche amministrazioni e degli operatori economici anche per gli acquisti sottosoglia, dall'altra, faciliterà la tempestiva adozione dei correttivi che si renderanno necessari[62].

Tra i dati statistici che possono essere oggetto di attenzione ci sono, in particolare, quelli relativi ad aspetti specifici delle figure apicali o agli amministratori dei soggetti coinvolti nelle procedure di gara (si pensi ai legami di parentela, ad eventuali incarichi politici ricoperti o alla titolarità di quote azionarie o partecipazioni in altre società), ai ribassi d'asta offerti o al dato storico dei tassi di partecipazione alle procedure di gara.

Originale è poi la previsione di grafici di relazioni che, utilizzando funzioni predittive e ricorrendo a tecniche di *Social Network Analysis*, siano in grado di individuare la costituzione di community di operatori economici al fine di evitare fenomeni che possano alterare il mercato e la concorrenza.

8.2. La sperimentazione di Sogei s.p.a.

Appare degno di nota soffermarsi, seppure brevemente per le esigenze di sintesi proprie del presente lavoro, sulla sperimentazione avviata da Sogei, società *in house* del Ministero dell'Economia e delle Finanze, con riguardo alla gestione della fase istruttoria e, nella specie, alle richieste di subappalto che si inseriscono all'interno delle procedure di gara.

Si tratta, a ben vedere, di un progetto che mira ad assistere l'ufficio legale nella procedura di verifica, in genere complessa e macchinosa, sulla sussistenza dei presupposti di legge e nelle conseguenti determinazioni da assumere nei confronti di un appaltatore che voglia ricorrere al subappalto.

La finalità è quella di automatizzare le fasi di lavorazione consentendo al contempo un controllo efficace e analitico sia in ordine alla mera sussistenza della documentazione indispensabile per gestire l'eventuale autorizzazione al subappalto, sia in ordine al suo contenuto e alla sua correttezza.

Il sistema di intelligenza artificiale basato sul *Natural Language Processing* (NLP) è la tecnologia che supporta i soggetti preposti al controllo e alla verifica della documentazione in grado di segnalare loro, tramite appositi sistemi di *alert*, la presenza di anomalie o di aspetti controversi.

Detta tecnologia, programmata sulla scorta delle specifiche finalità perseguite secondo la sperimentazione attivata da Sogei, prevede che l'appaltatore per via telematica debba, in particolare, produrre il contratto di subappalto contenente tutte le clausole espressamente richieste, nonché altra documentazione quale la dichiarazione dell'appaltatore e del subappaltatore, i richiesti certificati del casellario giudiziale, la dichiarazione antimafia e quella sostitutiva relativa all'iscrizione alla Camera di commercio[63].

Si tratta evidentemente di un'attività defatigante – caratterizzata da ripetitività e laboriosità – che richiede di verificare ogni allegato e firma digitale apposta con riguardo alla validità e all'effettivo potere di rappresentanza di chi abbia apposto la sottoscrizione, l'analisi approfondita del contenuto della documentazione prodotta e della conformità della situazione di fatto rispetto alle suddette dichiarazioni, nonché la valutazione di eventuali richieste di chiarimento o integrazione documentale.

Il modello sperimentato da Sogei è di supporto proprio con riguardo alla suddetta attività e – grazie a sistemi di intelligenza avanzata – favorisce un'analisi automatica e immediata della documentazione nel suo complesso con un risparmio di risorse e tempi, ma anche con una riduzione drastica del margine di errore.

Occorre, inoltre, soggiungere che l'analisi del contenuto dei documenti[64] viene facilitata dalla

62. Dati riportati nel documento Consip del 19 dicembre 2022 relativo alle attività di monitoraggio e rendicontazione per il PNRR.

63. L'iniziativa è stata illustrata a ForumPA, evento tenutosi a Roma al palazzo dei Congressi dal 21 al 23 maggio 2024.

64. Sul proprio portale Sogei ha pubblicato i documenti da produrre per ottenere l'autorizzazione al subappalto.

circostanza che gli operatori economici devono compilare dei modelli preimpostati.

Questa circostanza consente al sistema di intelligenza artificiale utilizzato di analizzare (*recte*: comprendere) più facilmente un testo.

L'interfaccia di validazione utilizzata, tra l'altro, consente all'operatore umano di apportare modifiche e correzioni o approvare del tutto l'analisi effettuata automaticamente.

Il citato modello, grazie al riconoscimento e alla lettura dei contenuti testuali, si rivela pertanto uno strumento fondamentale per la verifica di conformità dei documenti allegati e – consentendo di ottimizzare le attività portate avanti dall'ufficio – persegue obiettivi di ottimizzazione delle procedure di controllo

Sebbene la sperimentazione sia stata avviata con riguardo all'ipotesi di subappalto, ci si aspetta che i risultati incoraggiati già riscontrati – anche in ordine alla tempestiva acquisizione della documentazione integrativa rispetto ad un'allegazione che sia risultata incompleta – consentiranno di estenderne l'ambito di applicazione anche con riguardo ad altre attività.

Si pensi alla attività di protocollazione e conservazione delle comunicazioni pervenute, delle fatturazioni e dei pagamenti, e comunque all'acquisizione di dichiarazioni provenienti da soggetti esterni.

Le potenzialità di tale sperimentazione, del resto, dovranno essere sviluppate alla luce della considerazione che – quando sarà operativo il fascicolo virtuale dell'operatore economico e vi sarà piena interoperabilità dei sistemi con riguardo alla digitalizzazione all'intero ciclo di vita degli appalti pubblici – utilizzare un sistema di NLP[65] potrebbe consentire una verifica pressoché immediata sulle domande e sulla sussistenza dei requisiti di partecipazione alla procedura di evidenza pubblica.

Detto sistema di intelligenza artificiale avrebbe, cioè, un ruolo fondamentale anche nella fase di affidamento.

9. Il ricorso alla blockchain

Lo sviluppo della blockchain è sicuramente uno dei progetti più interessanti attualmente in fase di studio.

Essa, come è noto, è una tecnologia in grado di creare e gestire registri digitali distribuiti e sicuri. Nello specifico, tramite un registro decentralizzato e immutabile che tiene traccia delle c.d. transazioni in modo sicuro e trasparente, ciascuna informazione viene organizzata in blocchi collegati in modo crittografico. I vantaggi sono molteplici per sicurezza, conservazione e immutabilità, riservatezza e trasparenza dei dati, nonché per la prevenzione da eventuali manipolazioni[66].

La blockchain, pertanto, è una soluzione funzionale alla gestione delle infrastrutture digitali delle pubbliche amministrazioni in quanto agevola la conservazione e la certificazione delle informazioni.

Con riguardo poi alle procedure di gara, la realizzazione di una piattaforma verificata presenta ulteriori vantaggi del tutto evidenti dovuti alle circostanze che l'utilizzo di registri distribuiti risponde parimenti alle comuni esigenze di sicurezza, trasparenza, immutabilità. riservatezza e conservazione dei suddetti dati, ma è altresì in grado di preservare la concorrenza e il mercato.

È, peraltro, nella prospettiva della transizione digitale e della conseguente riforma del sistema nazionale di *e-Procurement* che il PNRR ha di fatto imposto l'implementazione dei sistemi di conservazione e certificazione dei dati immessi in occasione del coinvolgimento in procedure di appalto pubblico mediante il ricorso alla tecnologia blockchain.

All'uopo nel 2023 è stato avviato uno studio di fattibilità per individuare i supporti infrastrutturali e i requisiti di software che si rendano indispensabili per assicurare la conservazione di tutte le informazioni inserite nelle procedure di gara che orbitano sulla piattaforma Acquistinretepa.it.

Si tratta, a ben vedere, di un progetto pilota con finalità sperimentali che in prospettiva vuole estendersi ad altri ambiti e realizzare una rete infrastrutturale, fondata sulla tecnologia blockchain, per la conservazione e la certificazione dei dati per tutte le procedure di gara.

Al netto dello sforzo in termini di complessità organizzativa e infrastrutturale, nonché della rilevanza dei vincoli normativi relativi soprattutto alla

65. La nozione di NLP (*Natural Language Processing*) richiama algoritmi di intelligenza artificiale capaci di analizzare e comprendere il linguaggio naturale.

66. Magnuson 2020.

tutela della riservatezza e alla sicurezza dei dati, l'obiettivo è quello di realizzare un sistema che sia in possesso di specifiche funzionalità per la conservazione e la certificazione delle operazioni effettuate sulla predetta piattaforma.

Il complessivo efficientamento del sistema tramite il ricorso agli strumenti di crittografia più avanzati permette, tra l'altro, di ricostruire, in caso di guasti o anomalie, qual è stato il funzionamento della piattaforma nel corso della procedura di gara.

Con ciò favorendo il tracciamento delle procedure, l'immediata disponibilità dei dati e diminuendo potenzialmente il contenzioso dinanzi al giudice amministrativo con riguardo alle esclusioni dalle gare per il mancato invio della documentazione richiesta entro il termine prestabilito.

L'orientamento giurisprudenziale affermatosi al riguardo (Cons. Stato n. 7922/2019 e Cons. Stato n. 86/2020) ritiene, in particolare, che solo il malfunzionamento del sistema che abbia impedito il caricamento di detti documenti sia imputabile al gestore. Si profila, in tal modo, una distinzione tra rischio di rete e rischio di sistema secondo cui il primo consiste in un malfunzionamento tecnologico riconducibile a cali di efficienza della rete, mentre il secondo evoca un malfunzionamento della piattaforma di cui risponde la stazione appaltante.

Ebbene, con la realizzazione di un sistema fondato sulla tecnologia blockchain dei file log, ciascun interessato potrebbe acquisire le informazioni necessarie e ricostruire se si è trattato di un rischio di rete o di un rischio del sistema al fine di valutare se promuovere o meno un giudizio avverso il provvedimento di esclusione dalla gara in seguito a mancata trasmissione dei documenti richiesti sulla piattaforma digitale[67].

In proposito merita di essere altresì osservato che nell'eventuale giudizio può ritenersi assolto l'onere probatorio che incombe sulla stazione appaltante ove quest'ultima depositi semplicemente il file log del sistema contenente il report tecnico delle azioni compiute dall'operatore economico ricorrente all'interno della piattaforma digitale con riguardo al periodo di interesse.

Con riguardo al tema della tecnologia blockchain merita, inoltre, di essere analizzato quanto stabilito dall'art. 106 del d.lgs. n. 36/2023 rubricato "Garanzie per la partecipazione alla procedura".

Detto articolo, più in particolare, al comma 3, nel disciplinare le modalità tramite cui le garanzie fideiussorie debbano essere rilasciate, prevede che le stesse vadano emesse e firmate digitalmente, e che ciascuna di esse "deve essere altresì verificabile telematicamente presso l'emittente ovvero gestita mediante ricorso a piattaforme operanti con tecnologie basate su registri distribuiti".

Dal combinato disposto tra art. 30, già analizzato in precedenza, e il terzo comma dell'art. 106 in commento emerge, dunque, che si riconosce espressamente piena legittimità al ricorso alla tecnologia blockchain all'interno del sistema degli appalti pubblici. Le finalità sono quelle di implementare la trasparenza, l'efficienza e la certezza informatica.

Nello specifico si persegue l'obiettivo della dematerializzazione delle fideiussioni e della costruzione di un modello caratterizzato dall'interoperabilità dei sistemi su cui sono attivi i soggetti coinvolti nelle procedure di gara, nonché dalla condivisione della filiera dei processi e dall'automazione delle fasi di lavorazione con riferimento specifico alle verifiche di autenticità delle garanzie. Tale modello – nell'ottica di una piena affermazione della tutela della concorrenza – consente peraltro di avere un controllo più efficace verso possibili garanzie che risultino contraffatte.

La novella coinvolge, in particolare, gli operatori economici, le pubbliche amministrazioni, le stazioni appaltanti e gli enti concedenti, nonché le società assicurative e bancarie con riguardo a tutto il ciclo di vita del contratto di garanzia che si inserisce in una procedura di gara.

Sebbene si tratti esclusivamente di una parte delle fideiussioni emesse in favore delle pubbliche amministrazioni, è pur vero che la sperimentazione avviata con riguardo a quelle rilasciate nell'ambito dei contratti pubblici costituisce l'occasione per pensare ad un sistema più complesso che coinvolga tutti i contratti di garanzia.

Basti ricordare, a titolo esclusivamente esemplificativo, i contratti di fideiussione che vengono emessi con riferimento a taluni contributi agevolati o a fondo perduto, i rapporti scaturenti dagli oneri di urbanizzazione, le garanzie relazionate ai

67. Ghiani 2021.

rimborsi fiscali e a quelli che coinvolgono l'Agenzia delle Dogane per il pagamento dei diritti.

La prospettata interoperabilità dei sistemi, dunque, può sicuramente indurre le amministrazioni pubbliche ad avviare una generale rimodulazione complessiva dei processi interni, fermo restando la tutela dei dati personali acquisiti nel rispetto della disciplina europea e nazionale di riferimento.

In proposito va osservato che il Centro di ricerca su Tecnologie, Innovazione e servizi Finanziari dell'Università Cattolica di Milano sta portando avanti uno studio sui registri distribuiti in riferimento ai contratti di garanzia in collaborazione con attori pubblici, Banca d'Italia, Ivass, imprese, istituti bancari, società attive nel settore delle assicurazioni e Guardia di Finanza.

10. Proposte per il prossimo futuro

Alla luce di quanto suesposto e con riferimento specifico all'analisi della disciplina contenuta nel Codice dei contratti pubblici, si ritiene che – al fine di conseguire una maggiore efficienza in tutto il ciclo di vita delle procedure di gara – siano plurimi gli sviluppi che potrebbero coinvolgere le nuove tecnologie.

Il tema impone, in particolare, una riflessione sulla costituzione di sistemi interoperabili al fine di consentire l'acquisizione e lo scambio di informazioni di cui sono in possesso i soggetti coinvolti delle procedure di gara.

Basti pensare ai documenti prodotti e conservati dalle grandi centrali di committenza, ma anche alla banca dati istituita presso l'Anac contenente i fascicoli virtuali degli operatori economici.

Va al riguardo menzionato un applicativo, denominato *Price*[68], già sperimentato dalla Guardia di Finanza del Veneto per incrociare le informazioni acquisite da plurime banche dati.

Si tratta di un vero e proprio catalogatore di dati che, grazie alla notevole quantità di informazioni immesse e autonomamente analizzate, è in grado – tramite indicatori di rischio – di effettuare previsioni sugli operatori economici e di prevenire possibili illeciti.

Di fatto si tratta di un applicativo che acquisisce informazioni relativamente all'avvio di nuove attività, aperture di sedi, composizione del Consiglio di amministrazione e patrimonio sociale.

In generale si potrebbe ipotizzare di creare un supporto alla stazione appaltante e, nello specifico, al RUP mediante la previsione di un vero e proprio assistente virtuale in grado di coadiuvarlo nella attività che potenzialmente possono essere delegate a sistemi complessi fondati sulle nuove tecnologie, in particolare quelle che fanno ricorso a sistemi di riconoscimento del linguaggio, meccanismi di machine learning e reti neurali.

Tale supporto, che potrebbe accompagnare il RUP dalla fase di progettazione fino all'esecuzione del contratto, potrebbe riguardare in particolare l'attività di controllo e di verifica della documentazione acquisita segnalando anomalie e valutandone la coerenza.

In una prima fase sperimentale, con riguardo ai contratti pubblici, sarebbe poi possibile ragionare su singoli segmenti di attività, oppure esclusivamente su singole fasi.

Nella fase della programmazione i sistemi di intelligenza artificiale sono di fatto già in grado di effettuare indagini conoscitive sulla fornitura di un bene o sugli operatori che lo lavorano[69].

Tale attività preliminare è in grado di orientare la stazione appaltante nella fase di progettazione e nella predisposizione dell'elenco dei documenti e delle informazioni di cui ha bisogno. I sistemi di machine learning, tra l'altro, possono poi generare degli schemi relativi alla documentazione di gara, dai capitolati tecnici ai modelli di offerta.

Nella fase di affidamento, invece, sarebbe possibile utilizzare meccanismi di NLP per l'esame da parte della Commissione giudicatrice della documentazione prodotta.

Tale sistema, più in generale, è in grado di evidenziare e segnalare pressoché immediatamente la presenza di anomalie e difformità, ovvero la necessità di acquisire delle integrazioni documentali.

Basti pensare ad esempio all'irregolarità delle firme o alla mera verifica della sussistenza di taluni requisiti di partecipazione.

La fase esecutiva del rapporto negoziale, al fine di conseguire maggiore efficienza e celerità nell'esercizio della azione amministrativa, potrebbe, invece, essere segnata dall'introduzione degli

68. Si fa riferimento al protocollo d'intesa sottoscritto tra Regione Veneto e Guardia di Finanza l'8 febbraio 2022.

69. Gamero Casado 2023.

smart contract e dal ricorso a sistemi avanzati di intelligenza artificiale per le verifiche sugli stati di avanzamento, la rendicontazione delle spese e i pagamenti in un quadro contraddistinto dall'interoperabilità dei dati presenti nei database.

Tali piccole innovazioni sono in grado di apportare notevoli miglioramenti al ciclo di vita dei contratti pubblici in termini di risparmio e ottimizzazione delle risorse.

L'ambito che, tuttavia, a parere di chi scrive, offre maggiori potenzialità è quello relativo alla valutazione dell'offerta tecnica (oltreché economica) per la scelta del contraente.

Al riguardo è possibile rilevare che la stessa legge delega n. 78/2022 – che ha trovato attuazione con il d.lgs. n. 36/2023 – ha espressamente richiesto che venissero introdotti degli strumenti di automazione per la valutazione delle offerte da parte delle stazioni appaltanti[70] ed ha, pertanto, riconosciuto un ampio perimetro di azione alla commissione – presieduta dal consigliere di Stato Luigi Carbone – che ha lavorato al nuovo Codice.

11. Conclusioni

A cento anni dalla prima trasmissione radio, appare doveroso ricordare Guglielmo Marconi e l'intervento in cui tenne a precisare che "le invenzioni sono per salvare l'umanità, non per distruggerla"[71].

In attesa che siano adottate le nuove direttive europee sugli appalti pubblici, è tuttavia indubbio che il nuovo Codice contenuto nel d.lgs. n. 36/2023 offra al suo interno numerosi spunti interessanti e, per molti versi, capovolga le logiche sottese all'abrogato d.lgs. n. 50/2016.

Le spinte provenienti dal PNRR hanno, di fatto, imposto la transizione digitale nel settore della contrattualistica pubblica e indotto a recepire, almeno sul piano formale, l'invito ad investire sulle nuove tecnologie assumendo posizioni d'avanguardia relativamente alle quali storicamente le pubbliche amministrazioni di rado hanno saputo farsi interpreti.

Sebbene sia del tutto illusorio auspicare di poter irreggimentare, entro schemi predefiniti, ogni rischio scaturente dallo sviluppo delle nuove tecnologie (in particolare con riguardo ai sistemi generativi di intelligenza artificiale), è indubbio che – pur nella consapevolezza che si tratti di una fenomenologia che, al pari del moto ondoso, non sia governabile – esse rappresentino un'opportunità irrinunciabile.

È necessario, per tale ragione, chiarire quali obiettivi possa perseguire la pubblica amministrazione in termini di imparzialità e buon andamento ed investire, come si è diffusamente sottolineato, in un sistema di governance che individui adeguati presidi in grado di intervenire tempestivamente sia in via preventiva che successiva su eventuali errori o anomalie. L'osservanza dei principi su cui si fonda l'azione amministrativa, del resto, non può che collimare con la "riserva di umanità" che deve ispirare lo sviluppo delle nuove tecnologie.

Ciò, tuttavia, impone un duplice sforzo. In primo luogo, è necessario investire nella formazione del personale per fornirgli competenze adeguate in grado di padroneggiare i sistemi più evoluti e di coglierne, almeno potenzialmente, i rischi che derivano da un dataset incompleto o basato su elementi erronei in grado di alimentare ipotesi di discriminazione algoritmica.

In secondo luogo, è imprescindibile riflettere sul modello su cui strutturare un sistema di certificazioni che possa consentire all'agente umano di effettuare in maniera incisiva una penetrante attività di verifica e di controllo.

Le suggestioni che accompagnano lo studio dei meccanismi di apprendimento impongono, del resto, grande attenzione con riferimento alla conoscibilità e alla comprensibilità degli esiti forniti dai sistemi algoritmici ai fini della osservanza dei

70. L'art. 2 co. 2. lett. t della legge delega n. 78/2022 stabilisce. "individuazione delle ipotesi in cui le stazioni appaltanti possono ricorrere ad automatismi nella valutazione delle offerte e tipizzazione dei casi in cui le stazioni appaltanti possono ricorrere, ai fini dell'aggiudicazione, al solo criterio del prezzo o del costo, con possibilità di escludere, per i contratti che non abbiano carattere transfrontaliero, le offerte anomale determinate sulla base di meccanismi e metodi matematici, tenendo conto anche della specificità dei contratti nel settore dei beni culturali e prevedendo in ogni caso che i costi della manodopera e della sicurezza siano sempre scorporati dagli importi assoggettati a ribasso".

71. La frase è stata ricordata da Elettra Marconi, figlia dell'inventore della radio, in un'intervista trasmessa su RAI1 il 5 ottobre 2024.

principi di trasparenza e di ragionevolezza, nonché dell'obbligo di motivazione.

Solo un'applicazione concreta di quei principi potrà, infatti, consentire di trovare un punto di equilibrio tra regola matematica e regola giuridica scongiurando la denegata ipotesi che le nuove tecnologie non svolgano più una funzione strumentale e di supporto, ma siano addirittura artefici di ragionamenti autonomi dagli esiti imponderabili.

Sulla scorta di quanto testé esposto, le pubbliche amministrazioni devono, pertanto, essere consapevoli che sarà necessario predisporre adeguati strumenti per governare il fenomeno valorizzando un approccio collaborativo dei soggetti coinvolti al fine di consentire la conoscibilità degli algoritmi utilizzati, nonché di rafforzare i presidi di vigilanza e di controllo sia con riferimento ai modelli che alle competenze umane.

Sebbene le nuove tecnologie costituiscano un utile supporto anche per l'elaborazione delle griglie di sintesi nella scelta del contraente, è necessario assicurare che la riserva di umanità sia effettiva.

È, pertanto, fondamentale accertare che ogni fase del processo decisionale automatizzato sia tracciabile al fine di individuare facilmente il soggetto responsabile e ricostruire come è stata adottata una determinata decisione.

I nuovi scenari, del resto, impongono l'adozione di regole chiare per la progettazione, l'implementazione e l'uso delle tecnologie di intelligenza artificiale, garantendo – in virtù dei principi su richiamati – che i codici sorgente siano accessibili e ispezionabili anche da esperti indipendenti al fine di consentire la comprensione dei criteri utilizzati, nonché di effettuare ogni verifica su eventuali errori di selezione e valutazione.

Le amministrazioni pubbliche, tra l'altro, dovranno ragionare sulla previsione di audit periodici con esperti esterni riguardanti il corretto funzionamento dei modelli utilizzati.

È, invero, la previsione di un sistema di monitoraggio continuo che consente di intervenire tempestivamente sui malfunzionamenti e abusi, ovvero di ingenerare un legittimo affidamento negli stakeholders, negli operatori economici coinvolti nella procedura di evidenza pubblica, nonché nei fornitori delle tecnologie – interessati, peraltro, ad una adeguata protezione dei diritti di proprietà intellettuale sottostanti ai sistemi di intelligenza artificiale –.

Nondimeno il coinvolgimento di università o istituti di ricerca appare fondamentale nel processo di sviluppo di soluzioni basate sulla intelligenza artificiale.

È, dunque, con la predisposizione di strutture interne in seno alle stazioni appaltanti ed agli enti concedenti che siano in grado di presidiare adeguatamente le criticità evidenziate che sarà possibile promuovere adeguatamente lo sviluppo delle nuove tecnologie anche all'interno del microcosmo costituito dalla contrattualistica pubblica.

Riferimenti bibliografici

A. Amato Mangiameli (2022), *Intelligenza artificiale, big data e nuovi diritti*, in "Rivista italiana di informatica e diritto", 2022, n. 1

L. Avitabile (2017), *Il diritto davanti all'algoritmo*, in "Rivista italiana per le scienze giuridiche", vol. 8, 2017

M. Barberio (2023), *L'uso dell'intelligenza artificiale nell'art. 30 del d.lgs. 36/2023 alla prova dell'AI Act dell'Unione europea*, in "Rivista italiana di informatica e diritto", 2023, n. 2

M. Barberio (2023-a), *L'utilizzo degli algoritmi e l'intelligenza artificiale tra futuro prossimo e incertezza applicativa*, Aracne, 2023

E. Belisario, G. Cassano (2023), *Intelligenza artificiale per la pubblica amministrazione. Principi e regole del procedimento amministrativo algoritmico*, Giuffrè Francis Lefebvre, 2023

A. Bellini, A. Guidi (2022), *Python e machine learning*, O'Reilly Media, 2022

F. Caringella, L. Carbone, G. Rovelli (2024), *Manuale dei contratti pubblici*, Dike Giuridica, 2024

E. Carloni (a cura di) (2024), *Cittadini e pubbliche amministrazioni tra AI e diritto all'umano*, in "Rivista italiana di informatica e diritto", sezione monografica, 2024, n. 2

G. Cassano, E.M. Tripodi (2024), *Il Regolamento europeo sull'intelligenza artificiale*, Giappichelli, 2024

G. Cerrina Feroni, C. Fontana, E.C. Raffiotta (2022), *AI Anthology. Profili giuridici, economici e sociali dell'intelligenza artificiale*, il Mulino, 2022

A. Ciriello (2023), *La digitalizzazione della Giustizia tra presente e futuro*, in atti del convegno "Giornate di studi della Scuola Superiore della Magistratura" (Capri, 13-14 ottobre 2023), [s.n.], 2023

M. Clarich (2023), *Manuale di diritto amministrativo*, il Mulino, 2023

G. De Minico (2022), *L'amministrazione digitale: quotidiana efficienza e intelligenza delle scelte*, Editoriale Scientifica, 2022

E. Falletti (2022), *Discriminazione algoritmica*, Giappichelli, 2022

M. Farina (2023), *La proprietà intellettuale nell'era delle decisioni amministrative "artificiali": rischi di collisione?*, in "Rivista italiana di informatica e diritto", 2023, n. 1

G. Gallone (2023), *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo*, Wolters Kluwer, 2023

E. Gamero Casado (2023), *Inteligencia artificial y sector público*, Tirant lo Blanch, 2023

A. Ghiani (2021), *Blockchain: linee guida. Dai casi pratici alla regolamentazione*, Giappichelli, 2021

A. Lalli (a cura di) (2023), *La regolazione pubblica delle tecnologie digitali e dell'intelligenza artificiale*, Giappichelli, 2023

W. Magnuson (2020), *Blockchain Democracy: Technology, Law and the Rule of the Crowd*, Cambridge University Press, 2020

B.G. Mattarella (2024), *La digitalizzazione dei contratti pubblici nel nuovo codice*, Giappichelli, 2024

M. Mazzamuto (2020), *Santi Romano. L'ordinamento giuridico (1917-2017)*, Editoriale Scientifica, 2020

F. Merenda (2022), *Legalità, algoritmi e corruzione: le tecniche di intelligenza artificiale potrebbero essere utilizzate nel e per il sistema di prevenzione della corruzione?*, in "Rivista italiana di informatica e diritto", 2022, n. 2

B. Musti (2024), *I contratti a oggetto informatico*, Giuffrè Francis Lefebvre, 2024

A.G. Orofino (2022), La trasparenza oltre la crisi. Accesso, informatizzazione e controllo civico, Cacucci, 2022

A.G. Orofino (2008), *Forme elettroniche e procedimenti amministrativi*, Cacucci, 2008

M.G. Peluso (2023), *Intelligenza artificiale e tutela dei dati*, Giuffrè Francis Lefebvre, 2023

P. Perri, G. Ziccardi (a cura di) (2019), *Tecnologia e Diritto. I fondamenti di informatica per il giurista*, Giuffrè Francis Lefebvre, 2019

S. Pesucci (2022), *Diritto e intelligenza artificiale: opportunità e dilemmi nell'era della automazione*, in "Ristrutturazioni Aziendali", marzo 2022

F. Pizzetti (2018), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018

B. Romano (2018), *Algoritmo al potere. Calcolo giudizio pensiero*, Armando Editore, 2018

S. Rombi (2014), *L'accountability dei governi democratici. Una comparazione tra sette paesi europei*, Aracne, 2014

U. Ruffolo (2021), *XXVI lezioni di Diritto dell'intelligenza artificiale*, Giappichelli, 2021

U. Ruffolo (a cura di) (2020), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefebvre, 2020

S. Sapienza (2024), *Decisione algoritmiche e diritto*, Giuffrè Francis Lefebvre, 2024

A. Simoncini (2019), *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in "Rivista di BioDiritto", 2019, n. 1

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, S. Marchiafava (2023), *Sviluppi recenti in tema di Intelligenza Artificiale e diritto: una rassegna di legislazione, giurisprudenza e dottrina*, in "Rivista italiana di informatica e diritto", 2023

E. Tosi (2024), *Diritto privato delle nuove tecnologie digitali*, Giuffrè Francis Lefebvre, 2024

RIVISTA ITALIANA
DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0235 • articolo sottoposto a peer review • pubblicato in anteprima il 4 dic. 2025

Gino Fontana – Nicola Pierpaolo Barbuzzi

Profili giuridici degli agenti elettronici: smart contract, soggettività algoritmica e logiche computazionali

La pervasiva istituzionalizzazione dei sistemi decisionali autonomi e della normatività algoritmica scuote l'architettura giuridica tradizionale, sollevando questioni così profonde da rendere necessaria una revisione radicale del paradigma strutturale su cui si fonda l'ordinamento giuridico contemporaneo: possono gli algoritmi essere soggetti giuridici? Possono acquisire uno *status* normativo autonomo? La crescente delega dei processi decisionali all'IA complica la determinazione della responsabilità, poiché il funzionamento di questi sistemi, basato sull'apprendimento automatico e correlazioni statistiche, sfugge ai modelli classici di causalità giuridica. L'uso diffuso di contratti intelligenti basati su *blockchain* sposta l'enfasi dalla negoziazione alla codificazione automatica della volontà contrattuale, riducendo il margine di intervento *ex post* e trasformando la governance delle transazioni digitali. Emergono così nuove entità, gli *attanti algoritmici*, collocati tra la strumentalità tecnologica e l'autonomia operativa, dissolvendo la differenza epistemologica, sino ad allora granitica, tra soggetto e oggetto giuridico.

Contratti intelligenti – Soggettività algoritmica – Linguaggio macchinico – Ibridi – Attanti

Legal aspects of electronic agents: smart contract, algorithmic personhood, and computational logic

The progressive integration of autonomous decision-making systems and algorithmic rationalities is increasingly undermining the foundations of traditional legal frameworks, prompting a reconsideration of the paradigmatic structures underpinning contemporary legal orders. Can algorithms be legitimately regarded as legal subjects? Is it conceivable for them to acquire some form of normative autonomy? The growing delegation of decision-making to artificial intelligence complicates the attribution of legal responsibility, as these systems – driven by machine learning and statistical inference – operate beyond the reach of classical legal models of causation. Concurrently, the proliferation of blockchain-based smart contract is reshaping the contractual landscape: shifting emphasis from negotiation to automated execution and significantly limiting the scope for ex post legal intervention. This evolution gives rise to new entities – algorithmic actants – positioned ambiguously between technological tools and autonomous agents, thereby dissolving the long-standing epistemological boundary between legal subject and object.

Smart contract – Algorithmic subjectivity – Machine language – Hybrids – Actants

Gino Fontana, avvocato, PhD, è autore dei paragrafi 1, 2, 5; Nicola Pierpaolo Barbuzzi, docente a contratto di Diritto privato presso l'Universitas Mercatorum – Roma, PhD, avvocato, è autore dei paragrafi 3, 4, 6; l'abstract e la ricerca bibliografica sono stati realizzati da entrambi gli autori

1. Introduzione

Il digitale, che permea ogni aspetto della nostra quotidianità, ha profondamente mutato alcuni dei paradigmi tradizionali del diritto, imponendo una riflessione critica sulle nuove modalità d'interazione tra soggetti umani, dispositivi tecnologici e algoritmi. Nel contesto di una società sempre più digitalizzata, i sistemi auto-regolatori e il linguaggio macchinico o computazionale non si limitano più ad automatizzare processi complessi, ma introducono nuove forme di soggettività giuridica, ponendo all'interprete interrogativi inediti. Per rispondere all'inaspettata "autonomia" degli strumenti tecnologici, attesa l'interconnessione pervasiva tra tecnologie e processi giuridici, si rende necessaria la rimodellazione di alcune categorie giuridiche classiche, come quelle di "soggetto" e di "responsabilità". I soggetti giuridici digitali, come gli agenti software autonomi, rappresentano uno dei fenomeni più significativi di questa trasformazione. Essi, infatti, operano in contesti decentralizzati, spesso assumendo ruoli che tradizionalmente appartenevano agli esseri umani, come la negoziazione di contratti o la gestione di transazioni finanziarie. Sul punto, da anni, la dottrina si interroga sulla configurazione giuridica dell'algoritmo, non quale mero strumento tecnico, ma vero e proprio soggetto attivo del processo decisionale, capace, dunque, di modificare dinamicamente il quadro regolativo. Questo, spesso alimentato dall'Intelligenza Artificiale (AI), sfida il concetto tradizionale di soggettività poiché, pur non dotato di coscienza, agisce (in alcuni casi) in modo "autonomo" producendo effetti giuridicamente rilevanti[1]. La crescente autonomia degli agenti software pone interrogativi su questioni fondamentali relativamente al loro status privatistico e sulla responsabilità giuridica che deriva dalle loro "azioni". Si pone, ad esempio, la questione di chi debba essere ritenuto responsabile nell'ipotesi in cui un contratto intelligente (smart contract) venga stipulato a nome di un'entità umana o societaria e produca effetti giuridici tra le parti; una domanda, questa, al centro di un vivace dibattito dottrinale multidisciplinare che vede impegnati, e spesso contrapposti, filosofi del diritto, esperti di etica e giuristi.

Sebbene la materia si presenti ancora in uno stato embrionale, si possono sommariamente individuare due posizione contrapposte: quella di pensatori come Wroblewski e Fortuna[2], Irrgang[3], Floridi e Sanders[4] che negano la possibilità di considerare gli algoritmi degli agenti morali e, dunque, che non riconoscono loro alcuna "soggettività", e

1. Mazzuca 2024, pp. 241-264; Latzer–Mattern 2016.
2. Wróblewski–Fortuna 2023, pp. 29-48.
3. Irrgang 2006, pp. 2-16.
4. Floridi–Sanders 2004, pp. 349-379.

altri, come Wallach e Allen[5], Calo[6] o Coeckelberg[7] che, pur non attribuendo una soggettività morale di tipo tradizionale agli algoritmi, si dimostrano maggiormente disposti a tenere conto dell'autonomia delle loro decisioni e delle implicazioni delle loro azioni.

Indipendentemente dalle loro posizioni, le questioni teoriche legate alla responsabilità e all'autonomia degli algoritmi, così come elaborate da filosofi ed eticisti del diritto, influenzano sempre di più le pratiche legali, stimolando il pensiero giuridico e la prassi legislativa a ripensare le tradizionali categorie di soggettività, responsabilità e attribuzione dei diritti, richiedendo anche risposte sul piano normativo. Tanto trova ragione d'essere sulla considerazione della crescente interazione tra diritto e tecnologia, la quale, non solo cambierà *fortiori* le modalità di regolazione degli agenti artificiali, ma comporterà un'inevitabile evoluzione dei consolidati e rassicuranti paradigmi del diritto, obbligato nella teoria e nella prassi, ad accogliere le nascenti categorie giuridiche e le nuove forme di responsabilità. Sul punto, è significativo il contributo del teorico sociale del diritto Gunther Teubner, al quale si deve l'introduzione nel dibattito di nuovi soggetti di diritto, gli "ibridi" e gli "attanti", mutuati dalla teoria dell'attore-rete, i quali rimandano a entità capaci di interagire come intermediari nel tessuto digitale e di ampliare il concetto di soggettività, riconfigurando il concetto di persona giuridica[8]. La trasformazione della soggettività, secondo Teubner, si rivela fondamentale per comprendere e "trattare" la natura sociale dei nuovi attori collettivi emergenti come le "reti", sempre più protagonisti sulla scena globale. Gli "attanti", in tale contesto, come suggerisce il sociologo francese Bruno Latour, non possono essere considerati dei meri strumenti, ma come elementi co-costruttori delle relazioni sociali e normative, superando così quel limite che aveva Niklas Luhmann di applicare la teoria dell'agire collettivo ai "processori non umani"[9]. Gli "ibridi" e gli "attanti", tuttavia, non sono le uniche entità che, nella "intelligente" società algoritmica, sfidano i consolidati paradigmi del diritto. Non bisogna trascurare, infatti, il ruolo degli "attori collettivi" e degli "enti non umani", quali i DAO (Organizzazioni Autonome Decentralizzate) e gli algoritmi di *machine learning* che decostruiscono le tradizionali categorie del diritto societario e contrattuale, richiedendo una ridefinizione delle modalità d'imputazione della responsabilità[10]. Appare evidente come la governance algoritmica non sia più una necessità futura, ma immanente che impone soluzioni normative innovative non più differibili[11].

Imprescindibile, nel presente saggio, è la prospettiva regolativa incentrata sul "noi algoritmici" in cui la collaborazione tra soggetti umani e non umani si presenti come la *conditio sine qua non* per nuovi paradigmi sociali e normativi. È indubbio come la regolamentazione del rapporto tra esseri umani e sistemi algoritmici richieda un approccio interdisciplinare capace di integrare il diritto con la tecnologia, l'etica e la filosofia in quanto, come osservato da Hermendra Singh, "The governance of digital technologies involves a complex interplay of legal frameworks that aim to protect individual rights, ensure security, and promote ethical standards"[12]. Le categorie emergenti del diritto digitale delineano scenari in continua evoluzione, in cui le strutture normative tradizionali si confrontano con nuove forme di *agency* tecnologica e con una

5. Wallach–Allen 2008.
6. Calo 2015.
7. Coeckelberg 2020, pp. 4-20.
8. Teubner 2019.
9. Come spiega lo stesso Latour "La parola 'attante', tratta dal lessico della semiotica, consente di ampliare la problematica sociale sino a farvi rientrare tutti gli esseri che interagiscono all'interno di un'associazione e che si scambiano le rispettive proprietà", Latour 2002.
10. Le DAO, ad esempio, organizzazioni che operano senza una gestione umana diretta basandosi su *smart contract* eseguono automaticamente le decisioni prese collettivamente dagli *stakeholder*, sollevando, in caso di errori, abusi o conflitti di varia natura con le norme vigenti. Rigazio 2023, p. 686 ss.
11. Reviglio 2024, p. 412.
12. Singh 2024, p. 147.

ridefinizione delle dinamiche di imputazione della responsabilità. Sebbene molte di queste categorie siano ancora in fase di consolidamento teorico, il loro impatto sui rapporti tra automazione, soggettività giuridica e accountability è già tangibile, ridefinendo l'architettura regolativa del contemporaneo. L'obiettivo di questa riflessione è dunque quello di mappare le trasformazioni epistemologiche e operative che investono il diritto nell'era algoritmica, analizzando le tensioni tra normatività umana e computazionale. In un contesto in cui le infrastrutture digitali e i processi decisionali automatizzati si intrecciano sempre più con le logiche giuridiche, la sfida per le nuove generazioni di studiosi del diritto risiede nella capacità di promuovere un'interazione dinamica tra sapere giuridico e innovazione tecnologica, elaborando modelli regolativi capaci di rispondere alla complessità della governance algoritmica senza rinunciare ai principi fondativi della giustizia, della tutela dei diritti e della sostenibilità, estensivamente intesa.

2. Soggetti giuridici digitali nella società algoritmica degli smart contract

In passato la locuzione "società algoritmica" ha segnato "l'emergere congiunto, in senso alle società sviluppate, governate a partire dagli ultimi trent'anni del XX secolo dall'economia globalizzata, degli strumenti dell'informatica e del digitale, dell'intelligenza artificiale, delle reti e dei *big data*"[13], da qui la comparsa della cosiddetta *algoritmic society*, una nuova locuzione per indicare l'importanza crescente degli algoritmi, non solo con riferimento agli aspetti prettamente economici del capitalismo della conoscenza, ma anche ai loro riflessi su tutti gli aspetti del vivere civile, compreso quello del diritto. L'avvento della società algoritmica ha portato in superficie questioni di straordinaria significatività giuridica come la natura e lo status dei soggetti giuridici digitali; sotto la spinta dell'AI e dei sistemi di *machine learning*[14], come anticipato, sono stati introdotti nuovi "attori" che operano con autonomia decisionale, sollevando numerosi interrogativi sul loro inquadramento giuridico. La figura del soggetto giuridico digitale, infatti, è emersa come un elemento cruciale in un panorama dove agenti software, algoritmi e sistemi auto-regolatori agiscono non più come meri strumenti, ma come protagonisti sia nel processo decisionale che contrattuale. Rispetto a quanto osservato da Lazzini, per cui "…la macchina rispetto all'uomo non persegue un proprio interesse e, quindi, alla fine l'Intelligenza Artificiale è al servizio dei soggetti giuridici intesi in senso tradizionale"[15], la situazione, a parere degli scriventi, appare più sfumata e articolata, rimandando a questioni la cui soluzione sfugge a qualsiasi formula perentoria e, per certi aspetti, consolatoria.

Gli agenti software utilizzati per stipulare contratti digitali o per prendere decisioni economico-finanziarie, ad esempio, non rientrano in nessuna delle due principali categorie di soggetti giuridici, quali le persone fisiche e quelle giuridiche. Pur essendo stati programmati da esseri umani, infatti, gli agenti software operano in maniera "autonoma", analizzando grandi quantità di dati e adattandosi dinamicamente alle contingenze. Questa particolare forma di "autonomia", secondo alcuni, imporrebbe di riconsiderare le tradizionali categorie giuridiche in modo da includere anche i soggetti "non-umani", ritenendoli capaci di agire in modo "indipendente"[16], per altri, richiederebbe di operare, *a priori*, un distinguo tra automazione (che sarebbe una caratteristica degli smart contract) e autonomia (caratteristica più adeguata per l'AI)[17], mentre per altri ancora la questione andrebbe affrontata dalla prospettiva dell'attribuzione agli agenti software di uno "stato intenzionale"[18]. Gli algoritmi di ultima generazione, di fatto, non possono in alcun modo essere considerati strumenti passivi nelle mani degli esseri umani in quanto, in grado di influenzare profondamente il processo decisionale, determinando sempre più spesso le condizioni dei contratti, le offerte economiche

13. Ménissier 2022, p. 86.
14. Ruffolo 2019, pp. 109-128.
15. Lazzini 2022, p. 56.
16. Pagallo 2020, pp. 93-106.
17. Di Giovanni 2020, p. 260 ss.
18. Sartor 2003, p. 555 ss.

e persino le modalità di interazione tra le parti[19]. Gli smart contract, in particolare, esemplificano la complessità della soggettività algoritmica; se inseriti in una blockchain, infatti, sono auto-eseguibili (nel senso che applicano le condizioni contrattuali senza la necessità di un mediatore umano o una terza parte) e auto-*enforcing* (il che evita il rischio di doverli far rispettare) caratteristiche, queste, che dimostrano l'inessenzialità della presenza dell'elemento umano almeno nella parte esecutiva[20]. L'eventualità di attribuire una soggettività morale o giuridica a delle "entità" digitali[21] resta una questione altamente dibattuta[22] , rappresentando una delle prove più complesse per l'intera comunità scientifica. L'autonomia decisionale delle "entità" digitali e la loro influenza sulle dinamiche contrattuali ed economiche richiedono un ripensamento delle tradizionali categorie giuridiche, un obiettivo, questo, che può essere raggiunto solo attraverso un approccio multidisciplinare capace d'integrare filosofia, sociologia, etica e diritto in grado di prospettare soluzioni normative innovative per garantire una regolamentazione equa ed efficace.

3. Lo status privatistico degli agenti software autonomi

Gunther Teubner si è interrogato sulla possibilità di riconoscere agli agenti software autonomi, definiti come "una macchina capace di prendere decisioni autonome"[23], uno "status autonomo di diritto privato"[24]. Secondo l'autore, questa scelta comporterebbe una conseguenza inevitabile: "trattarli in toto come soggetti responsabili, oppure rassegnarsi a registrare un numero sempre crescente di 'incidenti' privi di un responsabile"[25]. La questione, tuttavia, appare di non facile soluzione e, soprattutto, non sembra potersi risolvere, semplicisticamente, come ritenuto da parte della letteratura giuridica[26] ed informatica [27], considerando gli agenti quali estensione dei "padroni umani" che resterebbero, pertanto, gli unici ai quali riconoscere lo status privatistico. Riferirsi all'autonomia degli agenti software accentua l'ossimoro insito nell'idea di considerare le macchine come agenti-soggetti. Tuttavia, è fondamentale precisare che, in questo contesto, l'autonomia non richiama la concezione kantiana di autodeterminazione morale, bensì assume una connotazione tecnologica e operativa, indicando la capacità degli agenti software di eseguire compiti specifici in modo indipendente, senza la necessità di un intervento umano continuo.

Di fatti, sono proprio alcune loro specificità che permettono di parlare di "autonomia" degli "agenti software", in grado di processare azioni basate su regole predefinite, su algoritmi di apprendimento o su analisi di dati in tempo reale; sebbene, dunque, le impostazioni siano progettate da programmatori umani, l'*iter* decisionale è finalizzato dal sistema senza più la necessità di un *input* esterno[28]. Lo stesso può dirsi per quei compiti, di complessità elevata, che richiedono analisi, pianificazione e interazione con altri sistemi, basandosi su obiettivi preimpostati, dimostrando la capacità di adattarsi a contesti dinamici, superando la mera esecuzione di istruzioni lineari. È il caso del *trading* finanziario[29] (in cui gli agenti software comprano/vendono azioni in base a modelli predittivi) o delle piattaforme di streaming o ancora delle *news feed* dei social in cui gli agenti software, grazie ad architetture di *machine learning*, senza la necessità di una

19. Engstrom–Ho 2020, pp. 800-854; Calo–Keats Citron 2021, pp. 797-845.
20. Szabo 1996, pp. 2-20.
21. Floridi–Sanders 2004-a, pp. 1-44; Wallach–Allen 2008.
22. Monateri 2024, pp. 269-300.
23. Teubner 2015.
24. Teubner 2019.
25. *Ibidem.*
26. Kirn–Müller-Hengstenberg 2015, p. 67; Bräutigam–Klindt 2015, pp. 137-142.
27. Spindler 2016, pp. 805-816.
28. Si pensi a un chatbot, dotato di AI, che può rispondere "autonomamente" a domande degli utenti, scegliendo la risposta migliore in base a una vasta base di dati e algoritmi di elaborazione del linguaggio naturale; Sammarco 2024.
29. Occhiuzzi 2019, pp. 391-400.

modifica del codice sorgente e quindi senza l'intervento umano successivo, sono in grado adattare il proprio sistema di raccomandazione imparando dalle preferenze dell'utente, aggiornando così la propria proposta sulla scorta delle precedenti interazioni[30].

I contesti complessi come la robotica, la domotica implementata dall'*Internet of Things* (IoT) e la cibersicurezza, il concetto di autonomia degli agenti software acquista una rilevanza sempre maggiore. Questa autonomia si basa sulla capacità di tali sistemi di raccogliere dati dall'ambiente circostante — sia esso fisico o digitale — per poi elaborarli ed eventualmente compiere azioni in modo automatico, senza la necessità di un intervento umano diretto[31]. Un esempio evidente si riscontra negli assistenti vocali e nei dispositivi IoT, che, dopo aver analizzato le informazioni ricevute, possono attivare autonomamente altri dispositivi connessi, come elettrodomestici, impianti di illuminazione, sistemi di sicurezza o sensori ambientali. In questi scenari, l'agente software non si limita a eseguire istruzioni preimpostate, ma esercita una forma di decisione autonoma, elaborando il contesto in tempo reale e interagendo in modo dinamico con l'ambiente e gli altri sistemi interconnessi.

L'autonomia implica anche una componente di proattività, ossia la capacità di avviare azioni senza la necessità di un *input* diretto da parte dell'operatore umano, anticipando bisogni (come nel caso di dosatori di farmaci) o risolvendo problemi di sicurezza bloccando, ad esempio, l'accesso ai server in caso di attacco informatico prima che l'agente umano possa intervenire[32]. Tuttavia, sebbene la "autonomia" operativa degli agenti software presenti profili di criticità concettuale, essa non implica un'indipendenza assoluta, poiché essi agiscono all'interno di limiti prestabiliti dai loro sviluppatori, come il codice, i dati a disposizione o i vincoli etici e legali imposti. Inoltre, essi non possiedono coscienza, intenzionalità né responsabilità morale e il loro funzionamento dipende da risorse esterne, come server, energia elettrica e accesso ai dati. Pertanto, la "autonomia" degli agenti software deve essere intesa in modo relativo, vincolata alle specifiche tecniche e alle condizioni di progettazione. Risulta, dunque, appropriato affermare come gli agenti software possano essere considerati "autonomi" non per la presenza di una volontà propria, ma per la capacità di eseguire compiti complessi e prendere decisioni operative in modo indipendente, nel rispetto dei limiti definiti dai loro progettisti; tanto pur rappresentando un punto di forza, non supera gli interrogativi iniziali in tema di responsabilità e soggettività[33].

Per il legislatore europeo[34] le problematiche legate alla responsabilità degli agenti software andrebbero risolte nel senso di imputare a questi responsabilità in virtù di un'autonomia data dalla sottrazione di una parte del loro agire al controllo umano. "Il diritto civile" spiega Teubner, "è posto in tal modo di fronte ad una alternativa: o riconoscere agli agenti software autonomi uno status giuridico indipendente, e trattarli in toto come soggetti responsabili, oppure rassegnarsi a registrare un numero sempre crescente di 'incidenti' privi di un responsabile. La dinamica della digitalizzazione produce senza sosta spazi vuoti, lacune di responsabilità, destinate ad ampliarsi sempre più in futuro"[35]. Ma cosa sono le "lacune di responsabilità" di natura tecnica? Secondo Teubner, queste consistono in una serie di disfunzioni che trovano origine, ad esempio, nella modalità collaborativa con cui i software vengono sviluppati da team di lavoro, nella dipendenza dell'accuratezza del codice (nonostante i controlli) da componenti hardware e software forniti da aziende esterne, o ancora nella progettazione di software predisposti a interagire in modi imprevedibili[36]. Diversamente, in senso giuridico, le lacune legate

30. Sassi 2019, pp. 109-128.
31. Luger–Rosner 2017, p. 196 ss.
32. Cardon–Itmi 2016, p. 26 ss.
33. Beckers–Teubner 2023.
34. Parlamento Europeo (Commissione affari giuridici), Progetto di relazione con raccomandazioni alla commissione per la regolazione civile nel campo della robotica (2015/21038(INL), 31 maggio 2016, p. 5 ss.
35. Matthias 2008, p. 111.
36. Teubner 2019.

agli agenti software sono il risultato di molteplici fattori come, ad esempio l'inadeguatezza dell'istituto della responsabilità civile[37] o le previsioni fallaci dovute all'utilizzo dei big data o alle dichiarazioni negoziali della macchina stessa[38]. Nel 2017 il Parlamento Europeo ha proposto "l'istituzione uno status giuridico specifico per i robot, di modo che almeno i robot autonomi più sofisticati possano essere considerati come persone elettroniche con diritti e obblighi specifici, compreso quello di risarcire qualsiasi danno da loro causato"[39], il tutto, però, nell'ottica di conquistare la fiducia dei cittadini utenti facendoli sentire tutelati e non minacciati dalle nuove tecnologie. Con questa finalità, la Commissione Europea, in una Comunicazione del 2019[40], ha ribadito l'importanza di considerare l'AI nei termini di uno strumento al servizio delle persone, rimarcando, in tal modo, la prospettiva antropocentrica della tecnologia[41]. Tutte le successive discussioni in seno al Parlamento e alla Commissione Europea, pur giungendo a normative importantissime in tema di AI e di robotica, hanno bypassato la questione di uno status giuridico *ad hoc* per i robot, per gli agenti software autonomi e per le AI. La questione dello status giuridico degli agenti software autonomi resta al centro di un vivace dibattito, polarizzato tra chi è pronto a riconoscere la piena soggettività giuridica[42] e chi continua a esprimere forti dubbi a riguardo[43]. Ad oggi, al netto della soluzione di preliminari questioni attinenti i diritti fondamentali[44], parte della dottrina, nel tentativo di trovare una soluzione di compromesso, in grado di superare l'*impasse*, ha proposto l'introduzione di un nuovo *genus* di soggettività, la "personalità elettronica".

Tuttavia, l'attribuzione di uno status privatistico agli agenti software autonomi è foriera di implicazioni complesse di natura contrattuale in quanto, la possibilità che questi possano negoziare contratti senza il ricorso all'intervento umano, pone interrogativi circa la validità giuridica e la fondatezza della responsabilità in caso di inadempimento, richiedendo una rivisitazione critica dei paradigmi tradizionali di capacità giuridica e responsabilità civile. Nei contratti tradizionali, la formazione del consenso è un elemento fondamentale dell'accordo, con il consenso espresso dalle parti attraverso dichiarazioni di volontà. Tuttavia, quando è l'agente software a operare autonomamente, si materializzano dilemmi giuridici di non facile soluzione, come, ad esempio, la questiono su chi rappresenti la volontà dell'agente e sul come assicurare che il suo agire rifletta le intenzioni del suo utilizzatore[45]. Altro problema attiene all'ipotesi d'inadempimento contrattuale, qualora un agente software non esegua un ordine o commetta un errore; in questo caso si potrebbe addebitare la responsabilità alternativamente al programmatore (se l'errore derivasse da un difetto nel codice), all'utilizzatore (nel caso non avesse configurato correttamente l'agente) oppure optare per una responsabilità diffusa di tutti i soggetti in azione. Anche nel campo della responsabilità civile, gli agenti software autonomi pongono sfide analoghe a quelle affrontate nei casi di automazione avanzata (si pensi al caso dei veicoli autonomi)[46] e sollevano numerosi interrogativi relativi, ad esempio, alla determinazione del nesso causale tra l'azione di un agente software e il danno subito da una parte o all'applicazione di concetti tradizionali come quelli della colpa o del dolo. Sul

37. Esemplare il caso citato da Jankowska–Pawelczyk–Kulawiak 2015, p. 88 ss.
38. Teubner 2019.
39. Parlamento Europeo, Relazione recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, Relazione–A80005/2017, 2015/2103(INL), 27 gennaio 2017.
40. Commissione Europea, Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Creare fiducia nell'intelligenza artificiale antropocentrica, COM (2019) 168.
41. Amidei 2019, pp. 1715-1726.
42. Zimmerman 2015, pp. 2-43; Wettig–Zehendner 2003, pp. 97-112; Allen–Widdison 1996, pp. 25-34.
43. Marshall 2023, pp. 1-3.
44. Gordon 2020, pp. 1-15; Solum 1992, pp. 1231-1287; Avila Negri 2021, pp. 1-11.
45. Teubner 2018, pp. 106-149.
46. Maio 2022.

punto, parte della dottrina propende per l'adozione di regimi di "responsabilità oggettiva", in cui il proprietario o l'utilizzatore dell'agente software risponde per i danni causati, indipendentemente dalla colpa[47].

In conclusione, la qualificazione privatistica degli agenti software autonomi si configura come un nodo concettuale di rilevanza interdisciplinare, la cui complessità assiologica richiede, ancora una volta, un approccio multidisciplinare. Sebbene permangano incertezze normative e interpretative, è evidente come l'ultima generazione delle "entità digitali" stia già determinando l'evoluzione dell'assetto giuridico, imponendo una revisione critica delle categorie tradizionali. L'evoluzione della biosfera in cui il diritto "vive", del resto, non può essere elusa *sine die*, poiché le problematiche emergenti esigono un inquadramento normativo e dogmatico in grado di far fronte alle sfide imposte dall'autonomia operativa degli agenti software.

4. "Ibridi" e "attanti": le nuove entità giuridiche nel diritto digitale

Come ampiamente argomentato, l'innovazione tecnologica ha introdotto nuove entità e strumenti che sfidano le tradizionali e consolidate categorie giuridiche, rendendo necessaria una riconsiderazione dei paradigmi normativi esistenti; i concetti di "ibridi" e di "attanti", derivati dalla filosofia e dalla teoria sociale, offrono una chiave interpretativa utile ad affrontare le questioni giuridiche sollevate dalla digitalizzazione, dall'intelligenza artificiale e dalla robotica. Il concetto di "ibrido" si riferisce a quelle entità che combinano elementi biologici e artificiali, materiali e immateriali, posizionandosi al di fuori delle tradizionali dicotomie giuridiche quali soggetto/oggetto o umano/non umano. Nel diritto digitale, tali entità operano con un certo grado di autonomia funzionale, pur rimanendo vincolate ai limiti imposti dal loro design, come nel caso dei robot autonomi impiegati in ambito sanitario: pur non essendo meri oggetti inanimati, non possono essere assimilati a soggetti di diritto dotati di piena capacità giuridica e responsabilità[48]. Uno degli aspetti più critici legati agli ibridi riguarda l'attribuzione della responsabilità giuridica per i danni, accidentalmente causati, dai loro processi decisionali. Le soluzioni ipotizzabili includono l'estensione della responsabilità ai soggetti che ne determinano il comportamento (sviluppatori, produttori, utenti), la creazione di nuove categorie normative intermedie o, come già anticipato, l'introduzione di una specifica personalità giuridica elettronica[49]. Il concetto di "attante", mutuato dalla teoria dell'*actor-network* di Bruno Latour, ridefinisce la tradizionale distinzione tra soggetti giuridici e oggetti, attribuendo a entrambi una capacità di incidere attivamente sulle dinamiche sociotecniche[50]. Nel contesto del diritto digitale, tale nozione consente di qualificare gli artefatti tecnologici come agenti dotati di una forma di *agency*, intesa come la capacità di influenzare processi decisionali e relazionali. Un attante può essere qualsiasi entità, umana o non umana, il cui operato modella le interazioni di una rete socio-tecnica; ad esempio, un algoritmo impiegato per l'assegnazione di prestiti bancari esercita un impatto determinante sugli esiti delle decisioni finanziarie, pur essendo il prodotto di un design umano[51]. Come avviene per gli ibridi, l'inquadramento degli attanti nel diritto digitale impone una revisione delle strutture normative esistenti, imponendo al legislatore di considerare le nuove variabili regolative legate alla coesistenza tra agenti umani e tecnologici[52]. In particolare, il funzionamento intrinsecamente opaco di alcuni attanti, come gli algoritmi di decisione automatizzata, solleva questioni di *accountability* e trasparenza[53], poiché i loro meccanismi interni operano spesso come "scatole nere", rendendo complessa l'identificazione dei criteri

47. Parlamento Europeo, Relazione recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, cit., punto 55; Chiappini 2022.
48. Polieri 2024, pp. 176-255.
49. Botero Arcila 2024, pp. 1-17.
50. Latour 2005.
51. Bontempi 2017, pp. 7-30.
52. O'Neil 2016; Zuboff 2019.
53. Barbuzzi 2024, pp. 170-179.

decisionali[54]. Inoltre, il rischio di *bias* algoritmici, derivante dall'uso di *dataset* incompleti o distorti, pone interrogativi circa le potenziali discriminazioni sistemiche perpetuate da tali tecnologie[55]. Per questa ragione, parte della dottrina ha avanzato la proposta di introdurre strumenti di certificazione etica[56] per garantire un maggiore controllo e verificabilità degli attanti digitali. Un esempio significativo dell'intersezione tra le categorie di ibridi e attanti è rappresentato dagli smart contract, i quali combinano elementi umani (come le clausole definite dalle parti contrattuali o dagli sviluppatori) e non umani (il codice eseguibile in modo autonomo). Nell'ottica latouriana, gli smart contract possono essere considerati quali attanti in quanto influenzano direttamente l'equilibrio contrattuale, determinando esiti che, nel diritto tradizionale, sarebbero stati frutto di negoziazione o dell'intervento di un'autorità terza. Sebbene gli ibridi e gli attanti derivino da matrici teoriche differenti, essi convergono nel superamento della dicotomia rigida tra umano e non umano, proponendo una visione più dinamica delle interazioni tecnologiche e delle responsabilità giuridiche[57]. Entrambi esercitano un'influenza autonoma, seppur entro limiti progettati dall'uomo, ponendo questioni centrali legate alla responsabilità, alla trasparenza e alla necessità di un adeguamento normativo. Ad esempio, un sistema di guida autonoma potrà essere qualificato sia come ibrido, per la sua integrazione tra elementi fisici e digitali, sia come attante, per il suo ruolo attivo nella gestione della sicurezza stradale[58]. Anche le sfide poste dall'emergere delle entità di ibridi e attanti richiedono, come ampiamente sottolineato, un approccio multidisciplinare in quanto l'adozione di tali categorie concettuali consentirebbe di ridefinire i paradigmi giuridici tradizionali legati, ad esempio, alla soggettività, offrendo nuovi strumenti interpretativi in grado di cogliere le trasformazioni indotte dalla digitalizzazione e dalla tecnologia. Tanto sarebbe in grado di affrontare, con una chiave di lettura innovativa, le problematiche legate alla responsabilità, all'*agency* e alla regolazione degli ecosistemi digitali, solcando la via per la formulazione di modelli normativi più flessibili ed in sintonia con le sfide imposte dalla immanenza tecnologica.

5. Attori collettivi ed enti *non* umani nel contesto giuridico contemporaneo

Le formazioni collettive (società, organizzazioni non governative e istituzioni pubbliche) rappresentano una categoria consolidata nell'ordinamento giuridico, dimostrando come il diritto abbia già affrontato e risolto la necessità di riconoscere soggettività a entità non individuali. Tali soggetti, dotati di personalità giuridica autonoma, possono acquisire diritti, assumere obblighi e agire in giudizio in maniera distinta rispetto ai singoli componenti che li costituiscono[59]. Come osservato da Teubner, gli attori collettivi sviluppano una propria identità istituzionale[60] e operano attraverso meccanismi di autoregolazione che li rendono portatori di interessi autonomi rispetto a quelli degli individui che li compongono. In tal senso, la loro responsabilità si configura come distinta e separata da quella dei membri, consentendo, ad esempio, a una società di rispondere per inadempimenti contrattuali senza che i soci siano direttamente coinvolti[61]. Inoltre, la loro persistenza nel tempo può superare di gran

54. Beckers–Teubner 2022.
55. Barbuzzi–Fontana 2024, pp. 421-450.
56. Martorana–Nutini 2024.
57. Fontana 2025.
58. Loh–Loh 2017, pp. 35-50.
59. Bennett Moses 2011, pp. 763-794.
60. Teubner parla degli attori collettivi in termini di corporate actor e scrive che "La qualità emergente di un corporate actor nasce solo da un'auto-descrizione nel sistema di azioni. Solo comunicazioni riflessive all'interno del sistema di azioni sulla loro stessa identità e capacità di agire costituiscono il corporate actor o il 'collettivo' come mero artefatto semantico, come un'idea condensata linguisticamente di identità di gruppo. Nella misura in cui un tale corporate actor viene istituzionalizzato, cioè si orienta effettivamente a questa autodescrizione nelle azioni organizzative, ottiene realtà sociale", Teubner 2019.
61. Lombardi 2020; D'Alessandro 1969.

lunga la durata della vita individuale dei componenti, come avviene nel caso delle multinazionali o delle ONG[62].

Un ambito di particolare rilevanza riguarda il riconoscimento giuridico degli enti artificiali[63]. L'evoluzione dell'intelligenza artificiale e della robotica avanzata introduce una nuova dimensione nel dibattito giuridico, sollevando interrogativi sulla loro collocazione normativa e sulla loro autonomia operativa. Sebbene tali sistemi non godano di personalità giuridica, il loro impiego solleva problematiche analoghe a quelle degli attori collettivi, soprattutto per quanto concerne la responsabilità e la necessità di un'infrastruttura regolativa che ne disciplini l'azione. Come gli attori collettivi, anche gli enti non umani richiedono un'intermediazione umana per operare nell'ordinamento e pongono questioni inedite sulla distribuzione della responsabilità, specialmente quando il loro comportamento produce effetti giuridici rilevanti[64]. La crescente autonomia di tali sistemi impone quindi un ripensamento dei modelli normativi tradizionali, al fine di adattarli a un contesto in continua evoluzione. Un'intelligenza artificiale avanzata può essere al contempo considerata parte di un attore collettivo, in quanto inserita in una rete sociotecnica, e un'entità autonoma, capace di incidere sul processo decisionale in modo non sempre prevedibile[65].

Il rapporto tra attori collettivi ed entità non umane, come algoritmi e sistemi di AI, costituisce una delle questioni più complesse nell'attuale riflessione giuridica e filosofica, poiché entrambi sfidano le categorie tradizionali della soggettività giuridica e della responsabilità. Mentre gli attori collettivi sono riconosciuti come soggetti di diritto, gli enti non umani operano in una zona grigia, privi di una qualificazione normativa univoca. Tuttavia, entrambi possono esercitare un'influenza diretta sul sistema sociale e giuridico, con effetti potenzialmente equiparabili. Se da un lato le persone giuridiche sono responsabili per le proprie azioni, dall'altro permane un'incertezza su come attribuire la responsabilità per le condotte di un'intelligenza artificiale o di un algoritmo che generano conseguenze dannose. Il problema si acuisce quando un attore collettivo fa uso di strumenti tecnologici autonomi: è il soggetto giuridico che li implementa a doverne rispondere integralmente, o occorre una ripartizione della responsabilità che coinvolga anche sviluppatori e fornitori? Per rispondere a tali criticità, alcuni studiosi hanno proposto di estendere ai sistemi di intelligenza artificiale modelli già applicati agli attori collettivi, ipotizzando l'introduzione di forme di personalità giuridica limitata o condizionata per specifiche applicazioni tecnologiche avanzate. L'approccio di Latour e della teoria dell'*actor-network* ha suggerito di concepire algoritmi e AI come attanti, riconoscendo loro una capacità di incidere sulle reti sociotecniche. Tale prospettiva consentirebbe una ripartizione della responsabilità tra gli attori collettivi che progettano e utilizzano questi strumenti e le entità non umane che ne determinano gli effetti. Un'ulteriore ipotesi normativa prevede un regime di co-responsabilità tra le due categorie, riconoscendo che entrambe concorrono alla produzione di determinati esiti giuridicamente rilevanti: ad esempio, un'impresa potrebbe essere chiamata a rispondere congiuntamente a un sistema AI mal progettato o a un algoritmo viziato da *bias* nei dati di addestramento. L'attribuzione della responsabilità giuridica agli attori collettivi che impiegano sistemi algoritmici risulta tuttavia complessa, poiché il funzionamento degli algoritmi si basa su processi opachi, spesso indecifrabili anche per i loro stessi sviluppatori. A differenza delle persone giuridiche, che operano secondo una volontà collettiva identificabile, gli algoritmi e le intelligenze artificiali non possiedono intenzionalità, ma eseguono operazioni secondo schemi predefiniti. Questo solleva il problema di stabilire se sia legittimo imputare loro

62. Teubner 2015.

63. Recentemente, sono stati riconosciuti dei diritti anche agli "enti naturali" come fiumi, montagne e foreste, trattandoli come soggetti giuridici; un approccio, questo, spesso definito "diritti della natura", che cerca di proteggere l'ambiente attribuendogli una forma di soggettività legale. Il fiume Whanganui in Nuova Zelanda è stato riconosciuto come persona giuridica nel 2017, con diritti e responsabilità legali proprie; O'Donnel–Talbot–Jones 2018, pp. 51-104.

64. Teubner 2015.

65. De Bona 2022.

una forma di responsabilità diretta o se, al contrario, questa debba necessariamente ricadere sugli attori collettivi che li controllano. Di conseguenza, il tema della responsabilità delle entità non naturali si articola in due dimensioni interdipendenti: da un lato, il riconoscimento dell'autonomia funzionale degli enti non umani; dall'altro, la necessità di garantire un sistema di *accountability* per le conseguenze derivanti dalla loro operatività[66].

L'integrazione giuridica di attori collettivi ed entità artificiali è destinata a diventare sempre più rilevante, spinta dalla necessità di regolamentare un contesto tecnologico in rapida trasformazione. In un mondo in cui la distinzione tra umano, naturale e artificiale si fa sempre più labile, il sistema normativo deve evolversi per assicurare un equilibrio tra innovazione tecnologica, tutela dei diritti e sostenibilità giuridica.

6. Prospettive per la regolamentazione della società dei "noi algoritmici"

La contemporaneità è segnata da un'interazione sempre più pervasiva tra esseri umani e algoritmi, dando origine a una configurazione sociale che alcuni definiscono "società dei noi algoritmici" [67]. In questo scenario, le decisioni individuali e collettive risultano spesso influenzate, se non direttamente plasmate, da processi automatizzati che incidono sulle dinamiche economiche, politiche e culturali. Gli algoritmi non possono più essere considerati meri strumenti esecutivi, in quanto operano come agenti attivi nella strutturazione delle relazioni sociali e nell'organizzazione del potere. La crescente autonomia di questi sistemi impone una riflessione approfondita sulla loro regolamentazione, che si configura come una delle sfide più urgenti del diritto contemporaneo. Rispetto alle epoche precedenti, la società algoritmica presenta caratteristiche peculiari che ne ridefiniscono le logiche operative. L'integrazione degli algoritmi è ormai ubiquitaria, trovando applicazione in ambiti eterogenei quali i social media, le piattaforme di commercio elettronico e le infrastrutture della governance pubblica. Attraverso tecniche di apprendimento automatico, i sistemi non si limitano a eseguire istruzioni predefinite, ma acquisiscono capacità di adattamento e auto-ottimizzazione, elaborando modelli predittivi su vasta scala. Tuttavia, il funzionamento di tali processi rimane opaco per la maggioranza degli utenti e, in taluni casi, persino per gli stessi sviluppatori, configurando il fenomeno della *black-box* AI. L'integrazione del *machine learning* negli smart contract segna un ulteriore avanzamento, delineando l'emergere di protocolli sempre più dinamici e adattivi, che ampliano le potenzialità applicative ma, al contempo, richiedono un impianto normativo capace di garantire trasparenza, *accountability* e giustiziabilità. L'urgenza di un quadro giuridico adeguato diventa dunque imprescindibile per armonizzare il progresso tecnologico con i principi fondamentali del diritto[68]. Tuttavia, la regolamentazione della società algoritmica solleva interrogativi di natura etico-giuridica che spaziano dalla trasparenza all'attribuzione della responsabilità, fino alla salvaguardia dei diritti fondamentali. Uno dei nodi più critici riguarda l'accessibilità e l'intelligibilità dei processi decisionali automatizzati: molteplici algoritmi sono sviluppati e implementati da enti privati, i quali tutelano i loro modelli come segreti industriali, rendendo arduo verificare l'equità e la non discriminatorietà delle decisioni. Il rischio di riproduzione e amplificazione di *bias* preesistenti nei dati di addestramento è particolarmente evidente nei sistemi di selezione del personale o di valutazione del merito creditizio, i quali possono perpetuare disuguaglianze strutturali in maniera automatizzata e sistemica[69].

Parallelamente, l'espansione delle capacità analitiche degli algoritmi ha intensificato le preoccupazioni in materia di tutela della privacy in quanto, l'elaborazione massiva di dati personali, spesso operata senza un adeguato controllo da parte degli interessati, potrebbe attingere le libertà individuali realizzando una vera e propria sorveglianza digitale[70]. Sul punto, il Regolamento Generale sulla

66. Teubner 2015.

67. Hardt–Mazumdar–Mendler-Dünner–Zrnic 2023.

68. Pasquale 2015.

69. Rahman–Ameen 2024.

70. Zuboff 2019.

Protezione dei Dati (GDPR) dell'Unione Europea ha rappresentato un significativo passo in avanti, ma la rapida evoluzione del contesto tecnologico rischia di renderlo insufficiente a fronteggiare le sfide emergenti. Per rispondere alle criticità della società algoritmica, sono state avanzate diverse proposte normative mirate a prevenire la perpetuazione di *bias* algoritmici e a limitare l'impiego di tali tecnologie nei processi decisionali ad alto impatto sulla vita delle persone, come l'accesso al credito o le procedure di assunzione. L'UNESCO, ad esempio, con la recente Raccomandazione sull'Etica dell'Intelligenza Artificiale, ha sottolineato l'importanza di standard internazionali per garantire un utilizzo responsabile degli algoritmi[71], mentre a livello europeo, la Commissione ha inteso adottare un approccio normativo flessibile, basato su una revisione periodica delle regolamentazioni e sull'introduzione di principi generali applicabili alle tecnologie emergenti. Anche il recentissimo AI Act[72] ha confermato questo trend, prevedendo l'istituzione di autorità indipendenti incaricate di supervisionare i sistemi algoritmici attraverso audit di conformità a standard etici e normativi, con la possibilità di irrogare sanzioni in caso di violazioni[73]. Tutte queste iniziative testimoniano la volontà di costruire un *framework* normativo capace di adattarsi alla continua trasformazione del panorama tecnologico, senza soffocare l'innovazione ma garantendo, al contempo, la protezione dei diritti fondamentali. La società dei "noi algoritmici" rappresenta una sfida inedita per il diritto, imponendo un ripensamento delle categorie giuridiche tradizionali e l'adozione di modelli regolativi innovativi. Gli algoritmi, con la loro capacità di influenzare scelte e relazioni sociali, non possono essere disciplinati secondo paradigmi normativi obsoleti. Una regolamentazione efficace dovrà dunque bilanciare la promozione dello sviluppo tecnologico con la necessità di preservare i principi di equità, responsabilità e trasparenza, garantendo una *governance* delle tecnologie algoritmiche che sia al servizio della collettività e non esclusivamente di interessi particolari.

7. Conclusioni

Gli effetti giuridici derivanti dall'impiego degli agenti elettronici, l'espansione esponenziale dei contratti intelligenti e il consolidarsi di concetti quali la soggettività algoritmica impongono una riflessione approfondita sulle implicazioni sistemiche dei processi auto-regolatori e del linguaggio computazionale nel quadro giuridico e sociale. L'analisi delle entità digitali nell'ecosistema algoritmico evidenzia con chiarezza come le tecnologie autonome basate sull'intelligenza artificiale stiano destabilizzando le categorie giuridiche tradizionali, disegnando scenari inediti e sollevando interrogativi cruciali sul modo in cui l'evoluzione tecnologica possa conciliarsi con i principi fondamentali del diritto, garantendo equità, *accountability* e trasparenza. L'incremento dell'autonomia operativa degli agenti software e la loro capacità di interagire con l'ambiente circostante pongono interrogativi inediti sulla loro qualificazione giuridica, generando un dibattito dottrinale e giurisprudenziale ancora privo di soluzioni univoche. La difficoltà di circoscrivere con precisione il grado di autodeterminazione, razionalità e capacità decisionale che potrebbe giustificare una forma di soggettività giuridica per queste entità evidenzia la necessità di ridefinire il rapporto tra tecnologia e responsabilità legale. Sebbene tali agenti non rientrino nelle tradizionali nozioni di soggetto di diritto, la loro integrazione nei contratti intelligenti e nei processi decisionali solleva l'urgenza di un adeguamento normativo in grado di disciplinare un quadro tecnologico dinamico ed in continua evoluzione. Un possibile orientamento potrebbe essere l'introduzione di una teoria della responsabilità algoritmica, incentrata sulla correlazione tra i soggetti coinvolti nella progettazione e nell'uso degli algoritmi. Un'alternativa consisterebbe nell'attribuzione di una personalità giuridica limitata agli agenti software, similmente a quanto avviene per determinate entità collettive,

71. Unesco, Raccomandazione. L'etica dell'IA: modellare il futuro delle nostre società, novembre 2023.

72. Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regolamento sull'intelligenza artificiale).

73. Raffiotta 2024.

conferendo loro diritti e obblighi specifici senza tuttavia assimilarli a persone fisiche o enti giuridici consolidati. Inoltre, l'affacciarsi di concetti quali "ibridi" e "attanti" nel diritto digitale testimonia la crescente complessità dell'interazione tra esseri umani e intelligenze artificiali, suggerendo una prospettiva più fluida rispetto al tradizionale binarismo soggetto-oggetto, che ha storicamente strutturato il diritto. La nozione di "ibrido" implica una commistione di elementi umani e non umani, richiedendo un ripensamento delle regole di attribuzione della responsabilità. Gli "attanti", invece, enfatizzano il ruolo attivo degli algoritmi in reti socio-tecniche, rendendo necessaria una visione giuridica capace di cogliere l'interconnessione tra differenti attori del sistema. Solo attraverso tale sinergia sarà possibile sviluppare strategie regolative efficaci e sostenibili. Gli smart contract rappresentano un caso emblematico del potenziale del linguaggio computazionale, consentendo l'automazione dell'esecuzione contrattuale, la riduzione dei costi e l'incremento dell'efficienza. Tuttavia, la rigidità intrinseca del codice informatico, incapace di adattarsi alle interpretazioni sfumate del diritto, costituisce una problematica rilevante, necessitando l'individuazione di un punto di equilibrio tra la prevedibilità e la cogenza automatizzata degli smart contract, da un lato, e l'esigenza di garantire equità e giustizia nei rapporti obbligatori, dall'altro. Inoltre, l'utilizzo crescente di algoritmi nei processi decisionali pone il problema della trasparenza e della verificabilità delle scelte automatizzate: la natura opaca di molte architetture algoritmiche ostacola la comprensione delle logiche sottostanti, rendendone difficoltosa la verifica della conformità ai principi giuridici. A tal fine, a parere degli scriventi, sarebbe opportuno istituire meccanismi di *audit* e certificazione degli algoritmi e incentivare lo sviluppo di intelligenze artificiali spiegabili (*Explainable* AI, XAI), al fine di garantire maggiore tracciabilità e *accountability* nei processi decisionali automatizzati.

Guardando alle prospettive future, la pervasiva integrazione degli algoritmi nei meccanismi sociali, economici e giuridici delinea un mutamento strutturale di portata inedita. La cosiddetta "società algoritmica" esige un impianto normativo dinamico e adattivo, fondato su una governance multilivello capace di coinvolgere attori istituzionali, esperti tecnici e società civile in un dialogo costante e interdisciplinare. Ad oggi, appare fondamentale orientare l'innovazione tecnologica secondo una prospettiva biocentrica, attenta al benessere collettivo, alla sostenibilità ambientale e sociale e alla tutela dei diritti fondamentali superando, di fatto, una limitante visione antropocentrica. Raggiungere tale equilibrio impone l'integrazione, *by design*, di principi etici nelle architetture algoritmiche e l'incremento della consapevolezza critica degli utenti rispetto all'impiego di tali strumenti; tuttavia, la padronanza concettuale può derivare esclusivamente da una solida cultura digitale, quale via privilegiata per disvelare quella "pareidolia semantica", che ci fa percepire "intenzionalità dove c'è solo statistica, significato dove c'è solo correlazione, comprensione dove c'è solo *pattern matching* su scala gigantesca"[74]. La costante diffusione degli smart contract, l'evoluzione della soggettività algoritmica e le questioni di responsabilità connesse all'automazione sollevano interrogativi giuridici di estrema attualità: se da un lato l'innovazione offre opportunità senza precedenti, dall'altro è essenziale gestire con rigore i rischi connessi all'impiego di sistemi decisionali autonomi. La definizione di un quadro regolatorio efficace, capace di armonizzare progresso tecnologico, cultura digitale e salvaguardia dei diritti, rappresenta una necessità inderogabile da affrontare, necessariamente, attraverso un approccio multisettoriale che coinvolga ed integri i diversi contesti del sapere. Sono queste le premesse sostanziali per la progettazione di un ecosistema algoritmico equo, trasparente e sostenibile.

Riferimenti bibliografici

T. Allen, R. Widdison (1996), *Can Computers Make Contracts?*, in "Harvard Journal of Law & Technology", vol. 9, 1996, n. 1

74. Floridi 2025.

A. Amidei (2019), *Intelligenza Artificiale e "product liability": sviluppi del diritto dell'Unione Europea*, in "Giurisprudenza italiana", 2019, n. 7

S.M.C. Avila Negri (2021), *Robot as Legal Person: Electronic Personhood in Robotics and Artificial Intelligence*, in "Frontiers in Robotics and AI", vol. 8, 2021

N. Barbuzzi (2024), *L'*accountability *nel sistema sanzionatorio del GDPR: oltre l'opacità del sistema*, in "Gazzetta forense", 2024, n. 2

N. Barbuzzi, G. Fontana (2024), *La responsabilità da trattamento algoritmico dei dati alla luce della normativa europea e della giurisprudenza comunitaria e italiana*, in "Rivista di Digital Politics", 2024, n. 2

A. Beckers, G. Teubner (2023), *Responsibility for Algorithmic Misconduct: Unity or Fragmentation of Liability regimes?*, in "Yale Journal of Law and Technology", special issue "Digital Public Sphere Series", vol. 25, 2023

A. Beckers, G. Teubner (2022), *Three Liability Regimes for Artificial Intelligence. Algorithmic Actants, Hybrids, Crowds*, Hart Publishing, 2022

L. Bennett Moses (2011), *Agents of Change: How the Law 'Copes' with Technological Change*, in "Griffith Law Review", vol. 20, 2011, n. 4

M. Bontempi (2017), *Reti di attanti. La concettualizzazione dell'agency e degli attori come effetti dei network nell'Actor-Network Theory*, in "Politica & Società", 2017, n. 1

B. Botero Arcila (2024), *AI liability in Europe: How does it complement risk regulation and deal with the problem of human oversight?*, in "Computer Law & Security Review", vol. 54, 2024

P. Bräutigam, T. Klindt (2015), *Industrie 4.0, das Internet der Dinge und das Recht*, in "Neue Juristische Wochenschrift", vol. 68, 2015, n. 16

R. Calo (2015), *The Good, The Bad and The Robot: Experts Are Trying to Make Machines Be "Moral"*, in "The Center for Internet and Society at Stanford Law School", 2015

R. Calo, D. Keats Citron (2021), *The Automated Administrative State: A Crisis of Legitimacy*, in "Emory Law Journal", vol. 70, 2021, n. 4

A. Cardon, M. Itmi (2016), *New Autonomous Systems*, Wiley-ISTE, 2016

D. Chiappini (2022), *Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione alla luce dell'Artificial Intelligence Act dell'Unione europea*, in "Rivista italiana di informatica e diritto", 2022, n. 2

M. Coeckelberg (2020), *Artificial Intelligence, Responsibility Attribution, and a Relational Justification of Explainability*, in "Science and Engineering Ethics", vol. 26, 2020

F. D'Alessandro (1969), *Persone giuridiche e analisi del linguaggio*, in Aa.Vv., "Studi in memoria di Tullio Ascarelli", tomo I, Giuffrè, 1969

G. De Bona (2022), *Verso la tutela giuridica dei sistemi intelligenti. Prospettive critiche della soggettività robotica*, in "Journal of Ethics and Legal Technologies", vol. 4, 2022, n. 2

F. Di Giovanni (2020), *Sui contratti delle macchine intelligenti*, in U. Ruffolo (a cura di), "Intelligenza artificiale. Il diritto, i diritti, l'etica", Giuffrè, 2020

D.F. Engstrom, D.E. Ho (2020), *Algorithmic Accountability in the Administrative State*, in "Yale Journal on Regulation", vol. 37, 2020, n. 3

L. Floridi (2025), *L'IA e la pareidolia semantica: quando vediamo coscienza dove non c'è*, in "Harvard Business Review Italia", giugno 2025

L. Floridi, J.W. Sanders (2004), *On the Morality of Artificial Agent*, in "Minds and Machines", vol. 14, 2004, n. 3

L. Floridi, J.W. Sanders (2004-a), *The method of abstraction*, in M. Negrotti (a cura di), "Yearbook of the Artificial. Nature, Culture & Technology", volume 2 "Models in Contemporary Sciences", Peter Lang, 2004

G. Fontana (2025), *Web scraping: Jurisprudence and legal doctrines*, in "The Journal of World Intellectual Property", vol. 28, 2025, n. 1

J.-S. Gordon (2020), *Artificial moral and legal personhood*, in "AI & Society", 2020

M. Hardt, E. Mazumdar, C. Mendler-Dünner, T. Zrnic (2023), *Algorithmic Collective Action in Machine Learning*, in A. Krause, E. Brunskill, K. Cho et al. (eds.) "Proceedings of the 40th International Conference on Machine Learning", JMLR.org, 2023

B. Irrgang (2006), *Ethical Acts in Robotics*, in "Ubiquity", 2006, September

M. Jankowska, M. Pawełczyk, M. Kulawiak (2015), *Legal personality and responsibility – a tale about how a robot does it alone in life*, in Id. (eds.), "AI: Law, Philosophy & Geoinformatics", Wydawnictwo Polskiej Fundacji Prawa Konkurencji i Regulacji Sektorowej Ius Publicum, 2015

S. Kirn, C.D. Müller-Hengstenberg (2015), *Technische und rechtliche Betrachtungen zur Autonomie kooperativ-intelligenter Softwareagenten*, in "Künstliche Intelligenz", vol. 29, 2015

B. Latour (2005), *Reassembling the Social. An Introduction to Actor-Network Theory*, Oxford University Press, 2005

B. Latour (2002), *Una sociologia senza oggetto? Note sull'intersoggettività*, in E. Landowski, G. Marrone (a cura di), "La società degli oggetti. Problemi di interoggettività", Meltemi, 2002

M. Latzer, F. Mattern (2016), *The Power of Algorithms – Tools or Actors?*, Center for Information Technology, and Law (ITSL), 2016

F. Lazzini (2022), *Etica digitale e Intelligenza Artificiale. I rischi per la protezione dei dati*, Giappichelli, 2022

W. Loh, J. Loh (2017), *Autonomy and Responsibility in Hybrid Systems: The Example of Autonomous Cars*, in P. Lin, K. Abney, R. Jenkins (eds.), "Robot ethics 2.0: From Autonomous Cars to Artificial Intelligence", Oxford University Press, 2017

R. Lombardi (2020), *Personalità e soggettività giuridica degli enti alla luce della Riforma del Terzo settore*, Giappichelli, 2020

E. Luger, G. Rosner (2017), *Considering the Privacy Design Issues Arising from Conversation s Platform*, in R. Leenes, R. van Brakel, S. Gutwirth, P. De Hert (eds.), "Data Protection and Privacy", Hart, 2017

E. Maio (2022), *Civil Liability and Autonomous Vehicles*, Edizioni Scientifiche Italiane, 2022

B. Marshall (2023), *No legal personhood for AI*, in "Patterns", vol. 4, 2023, n. 11

M. Martorana, G. Nutini (2024), *Algoretica: l'etica degli algoritmi nel futuro della tecnologia*, in Altalex, 2 ottobre 2024

A. Matthias (2008), Automaten als Träger von Rechten, Logos-Verlag, 2008

J. Mazzuca (2024), *L'intelligenza artificiale del diritto. Luci e ombre del ragionamento algoritmico*, in "Ragion pratica", vol. 62, 2024, n. 1

T. Ménissier (2022), *La servitù volontaria nella società algoritmica*, in "Filosofia politica", 2022

P.G. Monateri (2024), *Il walzer degli algoritmi e la responsabilità civile nell'era digitale*, in "Danno e responsabilità", vol. 29, 2024, n. 3

E. O'Donnel, J. Talbot-Jones (2018), *Creating legal rights for rivers: Lessons from Australia, New Zeland, and India,* in "Ecology and Society", vol. 23, 2018, n. 1

C. O'Neil (2016), *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown Publishing, 2016

B. Occhiuzzi (2019), *Algoritmi predittivi: alcune premesse metodologiche*, in "Diritto penale contemporaneo", 2019

U. Pagallo (2020), *Algoritmi e conoscibilità*, in "Rivista di filosofia del diritto", 2020, n. 1

F. Pasquale (2015), *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, 2015

P. Polieri (2024), *Gli agenti software e gli 'ibridi'. Dal paritetismo 'attanziale' umano/non-umano alla soggettività giuridica*, in "Euro-Balkan Law and Economics Review", 2024, n. 2

E. Raffiotta (2024), *I profili definitori e i principi dell'AI ACT*, in Aa.Vv., "Navigare l'european AI Act", a cura di AIRIA, Associazione per la Regolazione dell'Intelligenza Artificiale, Wolters Kluwer, 2024

A. Rahman, N. Ameen (2024), *Artificial Intelligence in HR Recruitment*, Archers & Elevators Publishing House, 2024

U. Reviglio (2024), *La regolazione dei sistemi di raccomandazione dei social media nell'Unione Europea*, in E. Brogi, M. Mariani (a cura di), "Temi di diritto dell'informazione e della comunicazione", Key editore, 2024

S. Rigazio (2023), *Lost in the Web: the Dark Sides of Smart Contracts. Except there Is Still Hope*, in "Opinio Juris in Comparatione", 2023, n. 1

U. Ruffolo (2019), *Intelligenza Artificiale, "machine learning" e responsabilità da algoritmo*, in "Giurisprudenza italiana", 2019, n. 7

P. Sammarco (2024), *Osservazioni sulla responsabilità da informazioni inesatte fornite da chatbot*, in "Il diritto dell'informazione e dell'informatica", 2024

G. Sartor (2003), *Gli agenti software e la disciplina giuridica degli strumenti cognitivi,* in "Il diritto dell'informazione e dell'informatica", 2003

S. Sassi (2019), *Gli algoritmi nelle decisioni pubbliche tra trasparenza e responsabilità*, in "Analisi giuridica dell'economia", 2019, n. 1

H. Singh (2024), *Legal Aspects of Digital Ethics in the Age of Artificial Intelligence*, in M. Pucelj, R. Bohinc (eds.), "Balancing Human Rights, Social Responsibility, and Digital Ethics", IGI Global, 2024

L.B. Solum (1992), *Legal Personhood for Artificial Intelligences,* in "North Carolina Law Review", vol. 70, 1992, n. 4

G. Spindler (2016), *Digitale Wirtschaft - analoges Recht: Braucht das BGB ein Update?*, in "Juristenzeitung", 2016

N. Szabo (1996), *Smart Contrats: Building Blocks for Digital Markets*, in "Extropy Journal of Transhumanist Thought", 1996

G. Teubner (2019), *Soggetti giuridici digitali? Sullo* status *privatistico degli agenti* software *autonomi*, Edizioni Scientifiche Italiane, 2019

G. Teubner (2018), *Digital Personhood? The Status of Autonomous Software Agents in Private Law*, in "Ancilla Iuris", 2018

G. Teubner (2015), *Ibridi e attanti, Attori collettivi ed enti non umani nella società e nel diritto*, Mimesis, 2015

W. Wallach, C. Allen (2008), *Moral Machine: Teaching Robots Right from Wrong*, Oxford University Press, 2008

S. Wettig, E. Zehendner (2003), *The Electronic Agent: A Legal Personality under German Law?*, in "Proceedings of the Law and Electronic Agents Workshop", 2003

Z. Wróblewski, P. Fortuna (2023), *Moral subjectivity and the moral status of artificial intelligence. A philosophical and psychological perspective*, in "Ethos", vol. 36, 2023, n. 4

E.J. Zimmerman (2015), *Machine Minds: Frontiers in Legal Personhood*, in SSRN, 2015

S. Zuboff (2019), *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2019

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0262 • articolo sottoposto a peer review • pubblicato in anteprima il 22 gen. 2026

Federica Scialoia

L'utilizzo di dati sanitari, *real-world data* e dati sintetici nello sviluppo di tecnologie sanitarie innovative nell'Unione europea

Il presente lavoro esplora le potenzialità dei dati sanitari nello sviluppo di tecnologie innovative, analizzando le possibili strategie per agevolare l'utilizzo di tali dati senza compromettere il diritto alla privacy dell'interessato. In particolare, l'indagine si soffermerà sull'importanza del trattamento di dati provenienti dal mondo reale per lo sviluppo di tecnologie sanitarie, in quanto più precisi e affidabili e dunque in grado di contribuire al miglioramento della salute dei pazienti. Tuttavia, trattandosi di dati sensibili ai sensi del GDPR è necessario il consenso dell'interessato al loro trattamento. Infine, vengono esaminate le possibili soluzioni per "anonimizzare" i dati sanitari, riflettendo sulla possibilità di introdurre una disciplina europea sui dati sintetici.

GDPR – Dati sanitari – Dati provenienti dal mondo reale – Tecnologie sanitarie – Dati sintetici

The use of health data, real-world data and synthetic data in the development of innovative health technologies in the European Union

This paper explores the potential of health data in the development of innovative technologies, analysing possible strategies to facilitate the use of such data without compromising the right to privacy of the data subject. In particular, the investigation will focus on the importance of real-world data processing for the development of healthcare technologies as more accurate and reliable and thus contributing to improved patient health. However, since it is sensitive data pursuant the GDPR, the consent of the data subject is required for their processing. Finally, are examined possible solutions for "anonymizing" health data, reflecting on the possibility of introducing a European discipline on synthetic data.

GDPR – Health data – Real-world data – Health technology – Synthetic data

L'Autrice è dottoressa di ricerca in diritto dell'Unione europea presso l'Università di Napoli "Parthenope"

1. Cenni introduttivi

Proteggere la salute e i diritti dei pazienti significa non soltanto garantire la sicurezza dei medicinali, dei dispositivi medici e in generale delle applicazioni tecnologiche impiegate nel settore sanitario, come previsto dall'art. 168, par. 4 TFUE[1], ma anche tutelare i dati sanitari dei pazienti trattati per lo sviluppo di tecnologie innovative. La maggior parte delle applicazioni tecnologiche come le terapie digitali[2] richiedono per il loro sviluppo il

1. Cfr. Oddenino 2010, p. 131 ss.; Fares–Campagna 2011, p. 325 ss.; Bestagno 2017-a, p. 119 ss.; Di Federico 2017, p. 664 ss.; Pesce 2021, p. 469 ss.; Bestagno 2017-b, p. 317 ss. In particolare, i "problemi comuni di sicurezza in materia di sanità pubblica, per quanto riguarda gli aspetti definiti nel presente trattato" rientrano nelle competenze concorrenti, come espressamente previsto dalla lett. k) del par. 2 dell'art. 4 TFUE. Nondimeno, siffatta competenza, attribuita nell'ambito esclusivo di intervento del par. 4 dell'art. 168 TFUE, si differenzia nettamente da quella che spetta all'Unione negli altri paragrafi del richiamato articolo, trattandosi, ai sensi dell'art. 2, par. 5, TFUE, di azioni intese a sostenere, coordinare o completare l'azione degli Stati membri, senza tuttavia potersi sostituire alla loro competenza, oppure come stabilito ai sensi del successivo art. 6, lett. a), TFUE, di azioni intese a sostenere, coordinare o completare l'azione degli Stati membri in settori quali la "tutela e il miglioramento della salute umana". È evidente, dunque, che tali ultimi articoli sono derogati dal citato par. 4 dell'art. 168 TFUE che, come noto, nelle altre ipotesi indicate, relega alla dimensione sovranazionale un ruolo di sostegno, coordinamento e completamento rispetto all'azione dei Paesi membri, rimanendo la "sanità", di cui al Titolo XIV del TFUE, declinata nell'art. 168, esclusa dall'elenco di cui all'art. 3 TFUE che stabilisce le competenze attribuite in modo esclusivo all'Ue. Tuttavia, si deroga a tale principio, solo per le misure ricomprese nell'alveo del par. 4 dell'art. 168 TFUE, attribuendo in tale settore all'Unione una competenza concorrente con quella degli Stati membri. Per esemplificare, nell'ambito delle misure circa organi e sostanze di origine umana, medicinali e dispositivi di impiego medico, nonché misure nei settori veterinario e fitosanitario, l'Unione si vede assegnate ben più significative, sebbene non esclusive, competenze, mentre nel quadro complessivo e generale dell'art. 168 TFUE essa può intervenire con azioni di mero completamento delle politiche interne degli Stati. Ciononostante autorevoli esponenti della dottrina hanno già avuto modo di precisare come sia necessario ridefinire i criteri di riparto delle competenze tra Stati membri e Unione in tale delicato settore, in tal senso vedi Rossi 2013, p. 749 ss.; Hodson–Maher 2018. Mentre per un commento della recente risoluzione del Parlamento europeo del 22 novembre 2023 sui progetti del Parlamento europeo intesi a modificare i trattati (2022/2051(INL)) vedi in particolare Adinolfi 2024, p. 8 ss.; Lazzerini 2023; Duff 2023, p. 9 ss.; Di Federico 2021-a, p. 71 ss.; Di Federico 2021-b, p. 8 ss.; Rinoldi 2022, p. 280.
2. Trattasi di applicazioni tecnologiche conosciute anche con l'acronimo *Dtx*, che deriva dal termine "*Digital Therapeutics*", utilizzato per indicare un settore specifico della sanità digitale quello relativo alle terapie digitali. In tale settore vengono ricomprese tutte quelle terapie effettuate tramite l'utilizzo di programmi software di alta qualità, supportati da evidenze scientifiche e cliniche. La possibilità di accedere ad una terapia digitale, tuttavia,

trattamento di dati personali con la conseguenza che il legislatore europeo dovrà fornire una duplice tutela: nei confronti dei destinatari di dette tecnologie e nei confronti dei fornitori di tali dati specie quando il trattamento venga effettuato da aziende private. In verità, già la comunicazione della Commissione europea del dicembre 2018[3] chiariva come lo sviluppo di sistemi di intelligenza artificiale non potesse trascendere dal quadro giuridico preesistente, in particolare, da quello posto a protezione dei dati personali[4]. Gli orientamenti del gruppo di esperti incaricati di elaborare i principi etici da rispettare per lo sviluppo dei sistemi di intelligenza artificiale mostravano un'attenzione specifica per la tutela dei dati personali precisando l'importanza di garantire la riservatezza e la protezione dei dati durante l'intero ciclo di vita del sistema[5], essendo a tal fine fondamentale l'intervento di un supervisore umano[6]. Questi ultimi aspetti ben evidenziati dal gruppo di esperti risultano peraltro presenti nella versione definitiva del testo del regolamento. Più concretamente, gli sviluppatori dovranno vagliare accuratamente la qualità, la natura, l'origine e la quantità di dati personali utilizzati, riducendo i dati inutili, ridondanti o marginali durante lo sviluppo e le fasi di addestramento e poi monitorare l'accuratezza del modello man mano che viene alimentato con nuovi dati[7]. Emerge pertanto una chiara intenzione delle istituzioni europee di regolare l'intelligenza artificiale senza pregiudicare i diritti fondamentali e, per quanto ci riguarda ai fini del prosieguo di questo scritto, della disciplina sulla protezione dei dati personali[8]. Senza soffermarsi in questa sede sulla struttura del regolamento sull'intelligenza artificiale che è stata ampiamente approfondita da molti esponenti

deve essere comunque valutata da un medico caso per caso e ciò avuto riguardo ad un'attenta disamina delle esigenze del paziente, prestando particolare attenzione sul livello di autonomia e di motivazione dello stesso. Non meno trascurabile pare la valutazione delle capacità tecnologiche di quest'ultimo per l'utilizzo dello strumento digitale in questione. Nondimeno, l'utilizzo delle *Dtx*, qualora ne sussistano i presupposti, potrebbe consentire l'identificazione precoce di eventuali ricadute di disturbi o malattie mediante il monitoraggio regolare dei sintomi e la valutazione dei progressi terapeutici, costituendo un valido strumento nelle mani tanto del medico quanto del paziente. Per un approfondimento esaustivo del tema in esame si rimanda a Scialoia 2024, p. 767 ss.; Salvatore 2023-b, p. 29 ss.

3. Comunicazione della Commissione *Piano coordinato sull'Intelligenza Artificiale*, 7 dicembre 2018, COM (2018) 795, preceduta, come noto, dalla Comunicazione della Commissione L'intelligenza artificiale per l'Europa, 25 aprile 2018, COM (2018) 237.
4. La Comunicazione della Commissione, *Piano coordinato sull'Intelligenza Artificiale* stabiliva che l'apertura ai flussi di dati internazionali dovrà continuare ad essere garantita nel pieno rispetto delle norme dell'Ue per la protezione dei dati personali e in conformità agli strumenti giuridici applicabili.
5. Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale istituito dalla Commissione europea nel giugno 2018, *Orientamenti etici per un'IA affidabile*, punto 72.
6. Il punto 65 degli *Orientamenti etici per un'IA affidabile* stabiliva che "la sorveglianza umana aiuta a garantire che un sistema di IA non comprometta l'autonomia umana o provochi altri effetti negativi. La sorveglianza può avvenire mediante meccanismi di governance che consentano un approccio con intervento umano (*human-in-the-loop* - HITL), con supervisione umana (*human-on-the-loop* - HOTL) o con controllo umano (*human-in-command* - HIC). L'approccio HITL prevede la possibilità di intervento umano in ogni ciclo decisionale del sistema, che in molti casi non è né possibile né auspicabile. L'approccio HOTL prevede l'intervento umano durante il ciclo di progettazione del sistema e il monitoraggio del funzionamento del sistema".
7. *Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108), approvato dal Consiglio d'Europa in occasione della riunione del 17 e 18 maggio 2018, ad Elsinore, in Danimarca. La Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione 108) è stata aperta alla firma a Strasburgo il 29 gennaio 1981.
8. Sul punto vedi Pollicino–De Gregorio 2021, p. 205 ss.; González de la Garza 2008, p. 62 ss.

della dottrina[9], basti qui ricordare che per il funzionamento di tali sistemi è necessario l'utilizzo di una grande mole di dati. Le modalità di raccolta e trattamento degli stessi, tuttavia, risultano assoggettate alla disciplina prevista dal regolamento 2016/679[10] il cui obiettivo è quello di bilanciare i vantaggi della sanità digitale rispetto ai rischi derivanti dalla divulgazione delle informazioni che discendono dal trattamento di dati sensibili. Il presente lavoro non ha l'obiettivo di ricostruire in maniera sistematica tutti gli aspetti relativi alla sanità digitalizzata, piuttosto, partendo dall'analisi dei dati sanitari come strumento utilizzabile per lo sviluppo di tecnologie altamente sofisticate in grado di contribuire al miglioramento della salute umana in conformità a quanto previsto dall'art. 35 della Carta dei diritti fondamentali dell'Unione europea[11], si propone di valutare l'apporto in tale settore dei meccanismi di "anonimizzazione", per sfuggire agli obblighi imposti dal GDPR senza pregiudicare il diritto alla protezione dei dati sanitari dei pazienti. Un'attenzione particolare sarà pertanto dedicata ai *real-world data* (di seguito nell'acronimo RWD) per tale intendendosi non una mera formula descrittiva bensì una categoria specifica di dati, corrispondente ai "dati provenienti dal mondo reale", al fine di renderli facilmente accessibili incrementando la loro disponibilità per finalità legate alla ricerca scientifica tramutandoli in "dati sintetici" e dunque anonimi.

2. Il trattamento dei dati sanitari alla luce del GDPR e le interazioni con il Regolamento sull'intelligenza artificiale

Occorre innanzitutto ricordare che la protezione dei dati personali è un diritto fondamentale che, ai sensi degli artt. 16 TFUE[12], 8 CDFUE[13], nonché dell'art. 8 CEDU[14], non ammette limitazioni a meno che non siano presenti scopi legittimi di natura medica e sanitaria, purché previsti dalla legge e solo nel caso in cui rispettino il contenuto essenziale di tale diritto e qualora siano proporzionati e necessari e dunque rispondenti a finalità di interesse generale riconosciute dall'Unione[15].

9. Vedi in particolare Carta 2024, p. 188 ss.; Inglese 2024; Rugani 2024; Zaccaroni 2024; Volpato 2024; Lattanzi 2024.
10. Per un commento vedi Fumagalli 2016, p. 1 ss.; Bassini 2016, p. 587 ss.; Mariottini 2016, p. 905 ss.; Ricci 2017; Cuffaro–D'Orazio–Ricciuto 2019.
11. In tal senso vedi Salvatore 2023-a, p. 3 ss.
12. "1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti. Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea."
13. Vedi in particolare González Fuster 2014, p. 198 ss. Pollicino–Bassini 2017, p. 134 ss.; Calzolaio 2017, p. 594 ss.
14. Sul punto si rimanda alla Corte EDU, sentenza 25 febbraio 1997, *Z. c. Finlandia*, ricorso n. 22009/93, punto 95, in cui si afferma che le legislazioni nazionali devono garantire la riservatezza dei dati sanitari ai sensi dell'art. 8 CEDU.
15. L'art. 52 CDFUE stabilisce che "1. Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. 2. I diritti riconosciuti dalla presente Carta per i quali i trattati prevedono disposizioni si esercitano alle condizioni e nei limiti dagli stessi definiti. 3. Laddove la presente Carta contenga diritti corrispondenti a quelli garantiti dalla Convenzione europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione. La presente disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa. 4. Laddove

Coerentemente alle richiamate norme di diritto primario, la disciplina prevista nell'ambito della direttiva 95/46/CE[16] viene modificata e sostituita dal più recente Regolamento Ue 679/2016, favorendo un innalzamento dello standard di protezione a livello nazionale essendo la normativa in esso contenuta direttamente applicabile. A ben vedere, il regolamento offre una nozione molto ampia di dati sanitari definiti come "dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute"[17]. Più specificamente, questi ultimi "comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio[18]; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro"[19]. Probabilmente l'intenzione del legislatore europeo nell'individuazione della nozione di "dati relativi alla salute" è quella di apprestare una tutela maggiore ai singoli, tuttavia, l'efficacia concreta della normativa in questione dipende dal contributo fornito da nuove figure professionali introdotte dal regolamento quali il titolare del trattamento e il responsabile del trattamento e dal rispetto dei principi che regolano la legislazione europea in materia di dati sanitari. Tra questi si annovera la "finalità" del trattamento, in quanto i dati personali e ancor più quelli sulla salute possono essere trattati solo nell'ambito delle finalità che si intendono perseguire[20] informando, in ogni caso, adeguatamente gli interessati[21]. In conformità al principio di "minimizzazione", inoltre, i dati devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati"[22]. Ad esempio, la documentazione in possesso di strutture pubbliche a scopi puramente amministrativi non dovrebbe contenere i parametri vitali del paziente in quanto tali aspetti appaiono superflui rispetto al profilo meramente gestionale[23]. Il trattamento dei dati sanitari inoltre è lecito soltanto nell'ipotesi in cui ricorrano le condizioni stabilite dal Regolamento. Invero, l'art. 6, par. 1 richiede il consenso dell'interessato, la necessità di proteggere i suoi interessi

la presente Carta riconosca i diritti fondamentali quali risultano dalle tradizioni costituzionali comuni agli Stati membri, tali diritti sono interpretati in armonia con dette tradizioni. 5. Le disposizioni della presente Carta che contengono dei principi possono essere attuate da atti legislativi e esecutivi adottati da istituzioni, organi e organismi dell'Unione e da atti di Stati membri allorché essi danno attuazione al diritto dell'Unione, nell'esercizio delle loro rispettive competenze. Esse possono essere invocate dinanzi a un giudice solo ai fini dell'interpretazione e del controllo di legalità di detti atti. 6. Si tiene pienamente conto delle legislazioni e prassi nazionali, come specificato nella presente Carta. 7. I giudici dell'Unione e degli Stati membri tengono nel debito conto le spiegazioni elaborate al fine di fornire orientamenti per l'interpretazione della presente Carta".

16. Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
17. Vedi art. 4, n. 14 del GDPR.
18. Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera.
19. Vedi considerando n. 35 del GDPR.
20. Nell'ambito sanitario le finalità possono essere principalmente di tre tipologie: di cura, di ricerca o amministrativo/contabili.
21. Strettamente collegati a detto principio sono i principi di proporzionalità, necessità, pertinenza e non eccedenza.
22. Vedi art. 5, par. 1, lettera c del GDPR.
23. Califano 2018, p. 20.

vitali o ancora l'esistenza di un interesse pubblico derivante dal trattamento. Prima di svolgere qualunque considerazione specificamente attinente al tema oggetto di indagine, è opportuno interrogarsi sulla figura del titolare del trattamento in quanto su quest'ultimo graverà, coerentemente con il principio di *accountability*, l'individuazione della base giuridica più idonea. Sappiamo infatti che quest'ultimo deve redigere un registro relativo alle attività di trattamento svolte sotto la propria responsabilità dovendo altresì adottare le misure tecniche e organizzative che risultino adeguate a garantire un livello di sicurezza adatto al rischio[24]. Detto obbligo è però esteso anche al responsabile del trattamento vale a dire "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali[25] per conto del titolare del trattamento"[26]. Nondimeno i maggiori problemi si riscontrano con riguardo all'esatta individuazione di quest'ultima figura, specie quando lo sviluppo delle tecnologie sanitarie richieda l'applicazione cumulativa del regolamento sull'intelligenza artificiale e del regolamento sulla protezione dei dati personali[27]. Invero, mentre quest'ultimo pone gli obblighi specifici suesposti in capo al titolare del trattamento, l'altra fonte derivata si sofferma invece esclusivamente sui "fornitori", con la conseguenza che nell'ambito dei sistemi di IA nel settore sanitario, non è facile comprendere chi debba rivestire la qualifica del "titolare del trattamento". Alcuni esponenti della dottrina hanno sostenuto che quest'ultimo debba coincidere con lo stesso sistema di intelligenza artificiale[28], detta impostazione appare tuttavia fuorviante in quanto finisce per dotare i sistemi di intelligenza artificiale di un'autonomia decisionale che

24. Art. 30 del GDPR.

25. Sulla definizione di dati personali si veda López Pina 2022, p. 51 ss.

26. Art. 4, par. 1, n. 8 del GDPR.

27. Vedi in particolare Contaldi 2021, p. 1203. Sebbene con riguardo specifico alla proposta di regolamento sull'intelligenza artificiale l'autore militi a favore della tesi che predilige l'approccio cumulativo di entrambe le fonti di diritto derivato. Invero dal momento che il regolamento sulla protezione dei dati mira a tutelare un diritto fondamentale previsto dalla normativa europea, i conflitti tra le due fonti normative non possono essere risolti in base al principio di specialità dovendo entrambe le fonti derivate applicarsi in maniera cumulativa. L'autore rileva inoltre che molte disposizioni, già presenti nella proposta di regolamento sull'intelligenza artificiale sembrerebbero deporre per la suddetta tesi. In particolare il considerando 24 il quale stabilisce che "qualsiasi trattamento di dati biometrici e di altri dati personali interessati dall'uso di sistemi di IA a fini di identificazione biometrica… dovrebbe *continuare a soddisfare tutti i requisiti derivanti dall'articolo 9, paragrafo 1, del regolamento (UE) 2016/679*". Oltre al considerando 72 che prevede che la creazione di spazi nei quali si procede a sviluppare ed istruire i sistemi di intelligenza artificiale debba avvenire tenendo conto delle prescrizioni dell'art. 6, paragrafo 4, del regolamento 2016/679 che stabilisce che "laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro: a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10; d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione". Per una puntuale disamina delle implicazioni derivanti dal trattamento dai dati personali rispetto alla proposta di regolamento sull'intelligenza artificiale vedi Resta 2022, p. 323 ss; Rossi Dal Pozzo 2020, p. 13 ss.

28. Simone 2020, p. 275 ss., p. 283.

prescinde da qualsiasi controllo umano[29]. Peraltro, dal dato testuale è possibile immediatamente escludere tale equiparazione non solo per il fatto che il regolamento sull'intelligenza artificiale non consente l'operatività di detti sistemi in maniera autonoma prevedendo sempre la necessità di un controllo umano, ma anche poiché lo stesso regolamento sulla protezione dei dati personali nell'individuare all'art. 4, par. 1 n. 7 i soggetti che potrebbero rivestire la qualifica di "titolare del trattamento" precisa che quest'ultimi possono coincidere con qualunque "persona fisica o giuridica, autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento". Sebbene il contenuto della disposizione appaia abbastanza ampio è comunque inequivocabile l'intenzione del legislatore di richiedere un minimo di personificazione per l'assunzione di tale veste. In tale prospettiva, lo stesso art. 22 del GDPR nello stabilire 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" sembrerebbe orientarsi per il riconoscimento di tale diritto al soggetto passivo che deve necessariamente coincidere con un individuo o un ente che abbia piena capacità giuridica, dotato dunque del potere di assumere decisioni in vece del sistema di IA[30]. Nell'attuale panorama regolatorio, deve pertanto negarsi la possibilità di concepire sistemi di IA totalmente automatizzati. Tale conclusione appare tanto più logica se si riflette sui profili di responsabilità derivanti dall'utilizzo di tecnologie particolarmente innovative nel settore sanitario. Così, soprattutto quando queste ultime siano fondate sull'utilizzo di sistemi di intelligenza artificiale sorge spontaneo chiedersi su chi debbano gravare gli obblighi discendenti dal GDPR nello sviluppo di tali tecnologie[31]. Verosimilmente la soluzione più appropriata sarebbe quella di rimettere in capo al fornitore il compito di rispettare le norme sulla protezione dei dati personali, dovendo nello sviluppo di dette applicazioni, attenersi anche agli obblighi imposti dal regolamento sull'intelligenza artificiale a seconda del "rischio" rispetto ai diritti fondamentali[32]. Più segnatamente, in conformità alle disposizioni del GDPR, quest'ultimo dovrà valutare attentamente i costi, la natura, l'oggetto, il contesto e la finalità del trattamento, avuto riguardo ai rischi potenziali per i diritti e le libertà dei singoli. L'onere probatorio relativo alla sicurezza del sistema incombe invece sulla stessa struttura, mentre sul titolare del trattamento grava la valutazione d'impatto sulla protezione dei dati sanitari[33],

29. Pizzetti 2018.

30. In tal senso Adinolfi 2020, p. 13 ss.

31. La letteratura riguardante il trattamento dei dati personali nello sviluppo di sistemi di intelligenza artificiale risulta molto ampia vedi in particolare Adinolfi–Simoncini 2022; Caggiano–Contaldi–Manzini 2024; Pajno–Donati–Perrucci 2022; Grieco 2023; Carta 2024, p. 188 ss.

32. L'Unione europea ha adottato una disciplina che non si basa sulle caratteristiche tecniche nell'utilizzo dell'intelligenza artificiale e dei suoi effetti ma sul sistema dei rischi collegati all'utilizzo di tali tecnologie. In quest'ottica, l'individuazione delle norme applicabili si fonda sulla ripartizione dei sistemi in quattro distinte categorie calibrate in base ai diversi fattori di "rischio". Nella prima categoria rientrano le applicazioni di IA i cui rischi risultano "inaccettabili". Tra queste, si annovera l'identificazione biometrica in tempo reale e gli algoritmi per il *social scoring*. Nella prospettiva dell'applicazione di tali sistemi al campo medico è interessante notare come tra le pratiche vietate siano incluse "l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta le vulnerabilità di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona che appartiene a tale gruppo in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico" vedi art. 5 lett. b. Tale previsione normativa tende a tutelare i pazienti che in contesti sanitari si trovino molto spesso in condizioni di vulnerabilità, potendo il loro comportamento essere distorto o influenzato.

33. Valutazione d'impatto sulla protezione dei dati (nell'acronimo DPIA, "*Data Protection Impact Assessment*"). Per una puntuale disamina del relativo meccanismo si rimanda a Hervey–Lavy 2020, p. 384. La procedura in questione è obbligatoria quando il trattamento possa "*presentare un rischio elevato per i diritti e le libertà delle*

potendo quest'ultima ai sensi dell'art. 35 del GDPR contenere l'esame di più trattamenti simili che presentino rischi analoghi. Per tutte le applicazioni tecnologiche che comportino un rischio particolarmente elevato l'art. 36 del GDPR prevede una preventiva consultazione con le organizzazioni dei pazienti e, se possibile, con i rispettivi garanti della protezione dei dati personali degli Stati membri[34].

3. L'attuale quadro normativo in materia di "real-world data"

Analizzate le linee essenziali della normativa relativa allo sviluppo di tecnologie innovative nel settore sanitario è possibile ora passare in rassegna la tipologia di dati sanitari che dovrebbero essere trattati per lo sviluppo di dette tecnologie. Non essendo qui dato analizzare tutte le tipologie di dati utilizzabili, si focalizzerà l'attenzione esclusivamente sui "real-world data" ciò in virtù del loro valore particolarmente significativo in termini di sicurezza ed efficacia del dispositivo. Occorre subito chiarire che trattandosi di dati generati da pazienti durante il loro percorso di cura e dunque direttamente desumibili dalla pratica clinica sono particolarmente precisi e accurati[35]. La loro eterogeneità consente infatti di ottenere informazioni aggiornate con riguardo al reperimento di evidenze scientifiche che andranno poi impiegate in procedimenti di HTA a livello di Unione[36] per lo sviluppo di nuove tecnologie. Saranno tuttavia utilizzati ai fini delle valutazioni cliniche congiunte esclusivamente i dati relativi al rischio/beneficio dei dispositivi escludendo qualsiasi valutazione di tipo economico/organizzativo e in relazione all'allocazione delle risorse. Ciononostante, nelle fasi di sviluppo dei farmaci e dei dispositivi medici la *real-world evidence* (RWE)[37] potrà fornire diverse e ulteriori informazioni in grado di migliorare le conoscenze in termini di efficacia, sicurezza e *compliance*. Con specifico riguardo allo sviluppo di medicinali è infatti evidente la crescente rilevanza di detti dati in quanto come precisato dall'EMA la maggior parte delle autorizzazioni di immissione in commercio rilasciate dagli enti regolatori conseguono alla valutazione dell'esistenza di prove di efficacia derivanti dal mondo reale[38]. L'uso della RWE per supportare il processo decisionale normativo non è però una novità. Sebbene tali dati siano stati utilizzati per decenni nella fase post-autorizzazione per valutare la sicurezza del medicinale, diversi studi ne apprezzano la rilevanza anche con riguardo al procedimento di valutazione[39]. Sul punto è bene precisare come il nuovo regolamento sullo spazio europeo dei dati sanitari[40], in linea con gli obiettivi tracciati dalla strategia europea in materia di dati[41], sembri orientarsi verso il riconoscimento del valore dell'uso di prove derivanti dal mondo reale per i processi decisionali correlati allo

persone fisiche". Va da sé, dunque, che la DPIA si differenzi dalla valutazione d'impatto prevista dal regolamento europeo sull'intelligenza artificiale *Fundamental Rights Impact Assessment*, di seguito "FRIA" per la maggiore specificità, non essendo rivolta alla totalità dei diritti fondamentali ma solo alla protezione dei dati personali.

34. Van Veen 2018, p. 70 ss.
35. Si tratta di dati provenienti da diverse fonti, tra cui database clinici, database amministrativi, registri di popolazione e di malattia, registri farmaceutici, cartelle cliniche elettroniche, *population health surveys* e dati di mobile *devices*, *wearable* e *apps*.
36. Regolamento (UE) 2021/2282 del Parlamento europeo e del Consiglio del 15 dicembre 2021 relativo alla valutazione delle tecnologie sanitarie e che modifica la direttiva 2011/24/UE. Per un approfondimento vedi Danieli 2023, p. 111 ss.
37. Con l'espressione *Real World Evidence* (RWE) deve intendersi l'analisi strutturata e organizzata di dati provenienti dalla reale pratica clinica (RWD), che consente di generare informazioni a integrazione delle evidenze prodotte dagli studi clinici sperimentali.
38. Flynn–Pluschke–Quinten et al. 2021, p. 90 ss.
39. Arlett–Kjær–Broich–Cooke 2022, p. 21 ss.
40. Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio, dell'11 febbraio 2025, sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847; per un commento della proposta di regolamento si veda Scialoia 2023.
41. Comunicazione della Commissione europea, *Una strategia europea per i dati*, COM (2020) 66.

sviluppo, all'autorizzazione e al monitoraggio non solo dei farmaci ma anche dei dispositivi medici e delle tecnologie digitali nel settore sanitario. Nello specifico, nell'individuare le categorie di dati sanitari elettronici che possono essere trattati per l'uso secondario, il regolamento include dati pertinenti provenienti dal sistema sanitario (cartelle cliniche elettroniche, dati relativi alle domande di rimborso, registri di malattia, dati genomici ecc.), dati che hanno un impatto sulla salute (ad esempio, consumo di varie sostanze, posizione socioeconomica, comportamento), inclusi i fattori ambientali (ad esempio, inquinamento, radiazioni, uso di determinate sostanze chimiche) e infine dati generati automaticamente provenienti da dispositivi medici o generati direttamente dalla persona attraverso applicazioni per il benessere[42]. Orbene, anche se nel regolamento non si rinvenga un espresso riferimento normativo ai dati provenienti dal mondo reale non introducendosi alcuna definizione in merito, dall'elenco di cui all'art. 33 è facile comprendere come esso si fondi esclusivamente sul riutilizzo di tale tipologia di dati[43]. Va da sé dunque ritenere che il dato proveniente dal mondo reale non sia limitato alla mera valutazione *ex post* del dispositivo in termini di sicurezza ed efficacia ma ben si estenda al procedimento normativo nel suo complesso. Pertanto, non è da trascurare il contributo che esso potrà avere in tutte le fasi del ciclo di vita della tecnologia e dunque anche nel supporto dell'iter valutativo dei farmaci. Le informazioni raccolte potrebbero infatti essere utilizzate dagli enti regolatori per monitorare costantemente il medicinale e valutare l'appropriatezza dell'intervento terapeutico nella pratica clinica. In conclusione può ritenersi che, pur creando le condizioni per il riutilizzo dei dati sanitari per finalità di ricerca attraverso una data governance condivisa, in vista dello sviluppo di trattamenti innovativi, le potenzialità dello spazio europeo dei dati sanitari, potrebbero essere migliorate, ad esempio, regolando e rendendo disponibili i RWD per disporre di informazioni integrative necessarie a rendere le prestazioni sanitarie più personalizzate. A tal fine, sarebbe auspicabile l'individuazione di definizioni chiare e condivise sulle varie tipologie di dati, essendo tuttora assente una nozione giuridicamente rilevante di *real-world data*. Oltre tutto non sembra trascurabile neppure l'obiettivo di armonizzare i criteri di accesso e gli standard di interoperabilità tra piattaforme individuando un meccanismo di partecipazione a livello di Unione in base al quale l'interessato presti il consenso all'uso secondario dei dati in un'ottica di GDPR *by design*, per evitare di dover richiedere il consenso ai singoli pazienti in un momento successivo alla progettazione del prodotto.

4. La nuova frontiera dei "dati sintetici"

L'analisi sin qui condotta lascia trasparire ancora talune ombre che devono dipanarsi. Benché sia soluzione condivisibile ritenere che spetti all'Unione europea intervenire sui richiamati profili per creare un connubio perfetto tra il modello europeo di protezione dei dati sanitari e la promozione del mercato digitale europeo, restano da chiarire le modalità operative per il raggiungimento di tale atteso risultato. Come anticipato, il regolamento sullo spazio europeo (EHDS) mira a facilitare l'accesso e la condivisione dei dati sanitari, promuovendo l'utilizzo di dati provenienti dal mondo reale. Fermo restando che il trattamento di tali dati è fondamentale per lo sviluppo di tecnologie sanitarie, occorrerebbe individuare la metodologia da

42. Vedi in particolare il considerando n. 39 del Regolamento sullo spazio europeo dei dati sanitari.

43. Vedi art. 33 del Regolamento sullo spazio europeo dei dati sanitari che elenca le categorie di dati sanitari elettronici per l'uso secondario inglobando: a) dati sanitari elettronici provenienti da cartelle cliniche elettroniche; b) dati su fattori con un'incidenza sulla salute, compresi i determinanti comportamentali, socioeconomici e ambientali della salute; c) dati sugli agenti patogeni pertinenti che incidono sulla salute umana; d) dati amministrativi relativi all'assistenza sanitaria, compresi i dati relativi alle domande di rimborso e ai rimborsi; e) estratti dei dati genetici, genomici e proteomici umani, quali i marcatori genetici; f) dati sanitari elettronici generati automaticamente mediante dispositivi medici; f bis) dati delle applicazioni per il benessere; g) dati identificativi relativi ai prestatori di assistenza sanitaria e alle categorie di professionisti sanitari coinvolti nella cura di una persona fisica o nella ricerca; j) dati sanitari elettronici provenienti da sperimentazioni cliniche soggetti alle disposizioni in materia di trasparenza a norma del diritto dell'Unione; l) dati derivanti da coorti di ricerca, questionari e indagini in materia di salute.

adottare per anonimizzarli conformemente ai requisiti normativi in materia di protezione dei dati personali. In particolare, ai sensi del considerando n. 26 del GDPR[44] se il dato è reso "anonimo" al punto tale da impedire o da non consentire più l'identificazione dell'interessato non si applicheranno le norme ivi contenute, con la conseguenza che l'adeguata anonimizzazione dei dati sanitari del paziente "a valle" consentirà di sfuggire agli adempimenti in materia di protezione dei dati personali, evitando *in toto* l'applicazione del GDPR[45]. La conseguenza più immediata di detto meccanismo è l'irrilevanza dell'art. 33 del regolamento sullo spazio europeo dei dati sanitari essendo superfluo il rifiuto dell'interessato, risultando pienamente garantita la sua riservatezza e il rispetto del principio di minimizzazione. L'analisi dei dati provenienti dal mondo reale come già precisato richiede necessariamente il consenso dell'interessato per il trattamento, trattandosi di dati sensibili, a meno che non si decida di tramutarli in "dati sintetici". Questi ultimi "sono dati artificiali generati da dati originali" attraverso "un modello che viene addestrato a riprodurre le caratteristiche e la struttura dei dati originali". Cosicché, i dati sintetici e i dati originali, se sottoposti alla medesima analisi statistica dovrebbero fornire, almeno in linea di massima, risultati molto simili. L'utilizzo di algoritmi di intelligenza artificiale per sintetizzare dati reali consentirà di creare nuovi dati che imiteranno quest'ultimi senza tuttavia contenere alcun elemento identificativo del paziente. Se adeguatamente generati non solo detti dati rifletteranno le caratteristiche di quelli reali ma renderanno impossibile ricondurre le relative informazioni a singoli pazienti. Per comprendere appieno il funzionamento dell'algoritmo che è alla base di detto meccanismo è opportuno riportare un esempio. Immaginiamo di avere a disposizione numerose informazioni riguardanti lo stato di salute dei pazienti di una clinica ospedaliera da cui si desumono i trattamenti che questi ultimi hanno ricevuto, i progressi compiuti, le eventuali patologie e i vari referti. Queste informazioni sono fondamentali per lo sviluppo di nuove tecnologie sanitarie in quanto indicano, qualora analizzate su larga scala, le patologie più comuni, l'età dei pazienti e tutta una serie di informazioni significative a fini statistici potendo orientare la ricerca scientifica e tecnologica nel settore sanitario. Senonché, trattandosi di dati sensibili richiederebbero ai sensi del GDPR il consenso degli interessati. Ma, se ipotizziamo di alimentare l'algoritmo di sintetizzazione con i suddetti dati, il risultato che otterremo riguarderà informazioni provenienti da una clinica ospedaliera di fatto inesistente con pazienti non riconducibili a quelli effettivi. Cionondimeno, le risposte derivanti dal database artificiale saranno statisticamente le medesime di quello reale, conducendo il procedimento di sintetizzazione alla creazione di nuovi dati, statisticamente equivalenti a quelli originali, ma differenti da quest'ultimi per l'anonimato degli interessati. Pertanto, nel settore sanitario i "dati sintetici" consentirebbero la condivisione di informazioni per finalità legate alla ricerca di nuove soluzioni diagnostiche e terapeutiche senza tuttavia esporre i pazienti a rischi di divulgazione dei propri dati sensibili e senza necessità di ottenere il preventivo consenso da parte di quest'ultimi per il trattamento degli stessi. Non a caso i dati sintetici si definiscono come dati "anonimizzati" e non "pseudonimizzati"[46]. Quest'ultima procedura infatti, sebbene dovrebbe essere utilizzata dai titolari del trattamento conformemente agli obblighi di cui all'art. 32 del GDPR[47], non esclude la "natura sensibile" dei dati trattati potendo attribuire

44. Per anonimizzazione si intende il processo volto a rendere anonimi i dati personali; i dati anonimi sono pertanto "le informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato".
45. In tal senso vedi Bolognini–Zipponi 2024.
46. Per un approfondimento delle differenze relative all'anonimizzazione e alla pseudonimizzazione vedi Agencia Española Protecciòn Datos e European Data Protection Supervisor, *10 Misunderstandings Related to Anonymisation,* 2021.
47. In base a tale norma il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la

all'individuo i dati cui si riferiscono attraverso l'utilizzo di informazioni aggiuntive[48], dovendo, pertanto, comunque applicarsi la normativa in materia di protezione dei dati personali. In conclusione, risulta di fondamentale importanza in un'ottica di classificazione del procedimento di sintetizzazione come tecnica di anonimizzazione differenziare quest'ultima rispetto alla pseudonimizzazione. Difatti, i dati sintetici appartengono alla prima categoria, e, qualora siano effettivamente anonimi ossia le relative informazioni non siano più riferibili al paziente, consentono di superare i limiti imposti dal GDPR offrendo nuove opportunità di utilizzo dei dati in sicurezza[49]. Del resto lo stesso regolamento (UE) 2024/1689 all'art. 59 prevede che quando i sistemi di IA siano impiegati per garantire la sicurezza pubblica e la sanità pubblica, compresi l'individuazione, la diagnosi, la prevenzione, il controllo e il trattamento delle malattie e il miglioramento dei sistemi sanitari i dati personali raccolti possono essere utilizzati per altre finalità[50]. Nel caso di sistemi ad alto rischio è preferibile tuttavia procedere al trattamento di dati anonimizzati, sintetici o di altri dati non personali. A ben vedere, la maggior parte dei sistemi impiegati nel settore sanitario rientrano in tale categoria e ciò non soltanto per la particolare destinazione d'uso dello strumento medicale per fini prevalentemente diagnostici e terapeutici[51], ma soprattutto per la sua qualificazione in termini di dispositivo medico. In base alla disciplina di cui al Regolamento MDR[52], devono ritenersi ad alto rischio tutti i dispositivi

capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

48. L'art. 4, par. 5, del GDPR definisce la pseudonimizzazione come "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".
49. In tal senso vedi Wiewiórowski 2021.
50. Vedi in particolare art. 59 lett. a).
51. L'Allegato III al punto 1, considera ad alto rischio "a) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche o per conto di autorità pubbliche per valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica essenziali, compresi i servizi di assistenza sanitaria, nonché per concedere, ridurre, revocare o recuperare tali prestazioni e servizi; d) i sistemi di IA destinati a essere utilizzati per valutare e classificare le chiamate di emergenza effettuate da persone fisiche o per inviare servizi di emergenza di primo soccorso o per stabilire priorità in merito all'invio di tali servizi, compresi polizia, vigili del fuoco e assistenza medica, nonché per i sistemi di selezione dei pazienti per quanto concerne l'assistenza sanitaria di emergenza". Occorre a tal proposito segnalare che mentre la citata letta a) menziona espressamente "autorità pubbliche" e "autorità private che operano per conto di autorità pubbliche", la lett. d) invece si limita a menzionare la tipologia del servizio indipendentemente dalla natura pubblica o privata del soggetto che lo eroga. In tal senso vedi Puigpelat 2023, p. 238 ss.
52. Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio.

medici e i dispositivi medico-diagnostici che sono sottoposti ad un controllo da parte di un organismo terzo. Di talché, non tutti i dispositivi medici rientrano nella categoria dei sistemi ad alto rischio ma solo quelli che richiedono una specifica valutazione di conformità. Per quelli che invece rientrano ai sensi del Regolamento (UE) 2017/745 nella classe I è sufficiente una mera autocertificazione[53], con la conseguenza che configurandosi quali applicazioni a basso rischio sono sottoposti a meri obblighi di auto-condotta. In base a tale logica i dispositivi indossabili come *smartwatch* – al di là della loro natura giuridica – non essendo sottoposti a specifici controlli da parte di organismi a ciò preposti non sono assoggettati alle regole previste per le applicazioni ad "alto rischio". Al contrario strumenti in grado di misurare i livelli di serotonina nel sangue dovrebbero qualificarsi a tutti gli effetti come dispositivi medici richiedendo, tra l'altro, l'intervento di un organismo di valutazione della conformità prima dell'immissione in commercio applicandosi tutti gli obblighi previsti dal regolamento sull'intelligenza artificiale per i sistemi ad alto rischio[54]. Dall'analisi delle norme del Regolamento sull'intelligenza artificiale emerge come la maggior parte dei sistemi di IA impiegati nel settore sanitario siano riconducibili a tale ultima categoria (alto rischio) con la conseguenza che, da un'interpretazione estensiva di tale disposizione si potrebbe concludere nel senso di ritenere che il legislatore europeo incentivi l'utilizzo nel settore sanitario di dati sintetici. D'altra parte occorre osservare che la lett. b) dell'art. 59[55], nel richiamare quest'ultima tipologia di dati equiparandoli a quelli anonimi e non personali, sembra confermare la natura giuridica "anonimizzata" di tali dati. Sta di fatto che i tentativi di regolazione tanto dei dati provenienti dal mondo reale quanto di quelli sintetici appaiono ancora troppo timidi. L'Unione europea dovrebbe sfruttare a pieno il potenziale della sintetizzazione dei dati, dacché quest'ultima se realizzata con adeguate metodologie, tutte ancora da definire, potrà garantire un giusto compromesso tra tutela e condivisione dei dati sanitari, mitigando i rischi di identificazione del paziente e supportando l'innovazione tecnologica nel settore sanitario, rappresentando pertanto un'idonea base per la futura costruzione del mercato unico della sanità digitale.

5. Possibili risvolti evolutivi di una disciplina europea in materia di dati sintetici

Sin dalle battute iniziali di questo breve scritto abbiamo avuto modo di precisare come l'utilizzo di dati sia fondamentale per lo sviluppo di tecnologie sanitarie. Benché le modalità di accesso e trattamento siano state già disciplinate dal legislatore europeo attraverso il GDPR appare altrettanto importante regolare in maniera dettagliata la tipologia di dati da trattare per lo sviluppo di tecnologie sanitarie innovative, essendo la salute un diritto fondamentale dell'Unione. Invero, l'art. 35 della Carta dei diritti fondamentali dell'Unione europea stabilisce che "ogni persona ha il diritto di accedere alla prevenzione sanitaria e di ottenere cure mediche alle condizioni stabilite dalle legislazioni e prassi nazionali", aggiungendo che nella definizione e nell'attuazione di tutte le politiche e le attività dell'Unione debba essere garantito "un livello elevato di protezione della salute umana". È dunque importante notare come il diritto alla salute venga inteso in un'accezione estensiva, dovendo essere tutelato non solo nei confronti dei cittadini europei ma di qualsiasi persona[56]. Nondimeno, è altrettanto fondamentale evidenziare come il diritto alla protezione dei dati personali sia ugualmente tutelato a livello di Unione, assurgendo a diritto fondamentale alla stregua di quello alla salute. Pertanto, essendo entrambi i diritti consacrati nella Carta dei diritti fondamentali dell'Unione europea occorrerebbe effettuare un bilanciamento tra gli stessi non potendo l'uno prevalere sull'altro. In attuazione del diritto alla salute sarebbe auspicabile

53. Kiseleva 2021. Gli obblighi sono disciplinati dal Capo II del regolamento, che fa espresso riferimento a doveri specifici di trasparenza e alla tutela dei diritti fondamentali.

54. Van Oirschot–Ooms, 2022, p. 10.

55. L'art. 59 lett. b) del regolamento sull'intelligenza artificiale stabilisce infatti che i dati trattati sono necessari per il rispetto di uno o più dei requisiti di cui al capo III, sezione 2, qualora tali requisiti non possano essere efficacemente soddisfatti mediante il trattamento di dati anonimizzati, sintetici o di altri dati non personali.

56. Salvatore 2021, p. 12.

incentivare l'utilizzo di dati provenienti dal mondo reale in quanto più affidabili e accurati e benché questi ultimi risultino oggetto di massima tutela da parte del GDPR per la loro natura "sensibile", ben potrebbero essere "anonimizzati" utilizzando nuove tecniche di intelligenza artificiale, tutelando parimenti il diritto alla protezione dei dati personali di cui all'art. 8 della Carta dei diritti fondamentali dell'Unione europea. Peraltro, nonostante l'analisi condotta si sia soffermata esclusivamente sugli aspetti positivi dell'utilizzo dei dati sintetici nell'ambito sanitario non possono di certo negarsi gli innumerevoli vantaggi del loro utilizzo anche in altri settori. Infatti sono ben noti i benefici dell'utilizzo di detti dati nel marketing e le relative ricadute rispetto alla disciplina consumeristica sia in termini di maggior efficienza del servizio erogato al consumatore che per il miglioramento delle strategie di marketing aziendale riducendo così i rischi di accesso a dati sensibili[57]. Come per il regolamento sull'intelligenza artificiale si potrebbe dunque riflettere sull'introduzione di una disciplina generale da applicare concretamente ai distinti settori materiali, incentivando l'utilizzo di meccanismi di "anonimizzazione" o di "pseudonimizzazione" a seconda del rischio rispetto alla protezione dei dati personali dell'interessato. Poiché la legislazione europea è per molti aspetti ancora *in itinere*, sarebbe auspicabile la modifica delle numerose proposte di atti normativi al fine di introdurre da un lato idonee procedure di valutazione e controllo delle tecnologie sanitarie per assicurare elevati standard di qualità e sicurezza e dall'altro meccanismi di trattamento dei dati sanitari volti a mitigare i rischi rispetto alla tutela della riservatezza dei pazienti. In definitiva, non può che rilevarsi come un intervento tempestivo del legislatore europeo in tale settore appaia non solo auspicabile ma ormai improcrastinabile.

Riferimenti bibliografici

A. Adinolfi (2024), *Le ragioni di una (incerta) riforma dei trattati dell'Unione*, in "Osservatorio sulle fonti", 2024

A. Adinolfi (2020), *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in S. Dorigo (a cura di), "Il ragionamento giuridico nell'era della intelligenza artificiale", Pacini Editore, 2020

A. Adinolfi, A. Simoncini (a cura di) (2022), *Protezione dei dati personali, e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Edizioni Scientifiche Italiane, 2022

P. Arlett, J. Kjær, K. Broich, E. Cooke (2022), *Real-World Evidence in EU Medicines Regulation: Enabling Use and Establishing Value*, in "Clinical Pharmacology & Therapeutics", 2022

M. Bassini (2016), *La svolta della "privacy" europea: il nuovo pacchetto sulla tutela dei dati personali*, in "Quaderni costituzionali", 2016

F. Bestagno (2017-a), *La tutela della salute tra competenze dell'Unione europea e degli Stati membri*, in L. Pineschi (a cura di), "La tutela della salute nel diritto internazionale ed europeo tra interessi globali e interessi particolari", Editoriale Scientifica, 2017

F. Bestagno (2017-b), *La tutela della salute tra competenze dell'Unione europea e degli Stati membri*, in "Studi sull'integrazione europea", 2017

L. Bolognini, S. Zipponi (2024), *Prospettive future in sanità spazio europeo dei dati sanitari e regolazione dei dati sintetici*, in L. Bolognini, S. Zipponi (a cura di), "Privacy e diritto dei dati sanitari", Giuffrè, 2024

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

57. Grisafi 2024, p. 155 ss.

L. Califano (2018), *Fascicolo sanitario elettronico (FSE) e dossier sanitario: il contributo del garante privacy al bilanciamento tra diritto alla salute e diritto alla protezione dei dati personali*, in G. De Vergottini, C. Bottari (a cura di), "La Sanità elettronica", Bologna University Press, 2018

S. Calzolaio (2017), *Protezione dei dati personali*, in "Digesto delle Discipline Pubblicistiche", Aggiornamento, Utet Giuridica, 2017

M. Carta (2024), *Il Regolamento UE sull'Intelligenza Artificiale: alcune questioni aperte*, in "Eurojus", 2024

G. Contaldi (2021), *Intelligenza artificiale e dati personali*, in "Ordine internazionale e diritti umani", 2021

V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di) (2019), *I dati personali nel diritto europeo*, Giappichelli, 2019

D. Danieli (2023), *Il nuovo Regolamento UE sulla valutazione delle tecnologie sanitarie: dal rafforzamento della cooperazione tra Stati membri al possibile impatto sul riparto delle competenze*, in V. Salvatore (a cura di), "Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea", Giappichelli, 2023

G. Di Federico (2017), *Protezione della salute*, in S. Allegrezza, R. Mastroianni, F. Pappalardo et al. (a cura di), "Carta dei diritti fondamentali dell'Unione europea", Giuffré, 2017

G. Di Federico (2021-a), *Il ruolo del Parlamento europeo nella costruzione del mercato unico digitale*, in G. Di Federico (a cura di), "Alla (ri)scoperta del Parlamento europeo. 1979-2019", Giappichelli, 2021

G. Di Federico (2021-b), *La strategia dell'Unione europea per i vaccini tra principio di attribuzione e leale collaborazione*, in "Eurojus", 2021

A. Duff (2023), *Five Surgical Strikes on the Treaties of the European Union*, in "European Papers", 2023, n. 1

G. Fares, M. Campagna (2011), *La tutela della salute nell'ordinamento comunitario*, in P. Gargiulo (a cura di), "Politica e diritti sociali nell'Unione europea. Quale modello sociale europeo?", Editoriale Scientifica, 2011

R. Flynn, K. Pluschke, C. Quinten et al. (2021), *Marketing Authorization Applications Made to the European Medicines Agency in 2018–2019: What was the Contribution of Real-World Evidence?*, in "Clinical Pharmacology & Therapeutics", 2021

M. Fumagalli (2016), *Le nuove normative europee sulla protezione dei dati personali*, in "Il Diritto comunitario e degli scambi internazionali", 2016

L.M. González de la Garza (2008), *Sociedad de la información en Europa*, Reus, 2008

G. González Fuster (2014), *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, 2014

C. Grieco (2023), *Intelligenza Artificiale e tutela degli utenti nel diritto dell'Unione europea*, Editoriale Scientifica, 2023

R. Grisafi (2024), *Il dato sintetico nell'approccio ermeneutico funzionale del diritto dei consumatori*, in S. Aracu, C. Rossi Chauvenet, L. Cristofaro (a cura di), "Paradisi artificiali. La nuova frontiera dei dati sintetici tra diritto e tecnologia", Aracne, 2024

M. Hervey, M. Lavy (2020), *The Law of Artificial Intelligence*, Sweet & Maxwell, 2020

D. Hodson, I. Maher (2018), *Eight Ideas for Reforming EU Treaty Making from Part III - The Practice of EU Treaty Making*, Cambridge University Press, 2018

M. Inglese (2024), *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno?*, in "Quaderni AISDUE", 2024

A. Kiseleva (2021), *AI as a Medical Device: Between the Medical Devices Framework and the General AI Regulation, Time to Reshape the Digital Society. 40th Anniversary of the CRIDS*, in "SSRN", 2021

S. Lattanzi (2024), *Prime riflessioni sull'applicazione del nuovo regolamento sull'intelligenza artificiale al settore sanitario*, in "Quaderni AISDUE", 2024

N. Lazzerini (2023), *La risoluzione del 22 novembre 2023 del Parlamento europeo sui progetti di modifica dei Trattati nel contesto delle prospettive di riforma dell'Unione (3/2023)*, in "Osservatorio sulle fonti", 2023, n. 3

A. López Pina (2022), *El Derecho ante el reto de la transformación digital*, Editorial Aranzadi, 2022

C.M. Mariottini (2016), *Il pacchetto di riforma della Commissione europea in materia di protezione dei dati personali*, in "Rivista di diritto internazionale privato e processuale", 2016

A. Oddenino (2010), *Profili internazionali ed europei del diritto alla salute*, in R. Ferrara (a cura di), Salute e sanità, in "Trattato di biodiritto", diretto da S. Rodotà e P. Zatti, Giuffrè, 2010

A. Pajno, F. Donati, A. Perrucci (a cura di) (2022), *Intelligenza artificiale e diritto: una rivoluzione?* Vol. I, *Diritti fondamentali, dati personali e regolazione*, il Mulino, 2022

C. Pesce (2021), *Sanità*, in P. De Pasquale, F. Ferraro (a cura di), "Manuale di diritto dell'Unione europea di Giuseppe Tesauro", II, Editoriale Scientifica, 2021

F. Pizzetti (2018), *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in F. Pizzetti (a cura di), "Intelligenza artificiale, protezione dei dati personali e regolazione", Giappichelli, 2018

O. Pollicino, G. De Gregorio (2021), *The principle of the rule of law in the regulation of AI*, Wolters Kluwer, 2021

O. Pollicino, M. Bassini (2017), *Art. 8. Protezione dei dati personali*, in S. Allegrezza, R. Mastroianni, F. Pappalardo et al. (a cura di), "Carta dei diritti fondamentali dell'Unione europea" Giuffrè, 2017

O.M. Puigpelat (2023), *The impact of the AI Act on public authorities and on administrative procedures*, in "Rivista interdisciplinare sul diritto delle amministrazioni pubbliche", vol. 4, 2023

G. Resta (2022), *Cosa c'è di "europeo" nella proposta di regolamento UE sull'Intelligenza Artificiale?*, in "Diritto dell'informazione e dell'informatica", 2022

A. Ricci (2017), *I diritti dell'interessato*, in G. Finocchiaro (a cura di), "Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali", Zanichelli, 2017

D. Rinoldi (2022), *«In deroga… e in conformità»: prospettive dell'Unione europea della salute muovendo dall'art. 168 TFUE per andar ben oltre (verso un comparto sanitario federale continentale?)*, in "Corti Supreme e Salute", 2022

L.S. Rossi (2013), *L'Unione Europea e il paradosso di Zenone. Riflessioni sulla necessità di una revisione del Trattato di Lisbona*, in "Il Diritto dell'Unione Europea", 2013

F. Rossi Dal Pozzo (a cura di) (2020), *Mercato unico digitale, dati personali e diritti fondamentali*, in "Eurojus", 2020

G. Rugani (2024), *La promozione di strumenti di coregolazione dell'intelligenza artificiale nell'AI Act, con particolare riferimento alle* regulatory sandboxes, in "Quaderni AISDUE", 2024

V. Salvatore (2023-a), *L'Unione europea disciplina l'impiego dell'intelligenza artificiale e dei processi di digitalizzazione anche al fine di promuovere la tutela della salute*, in V. Salvatore (a cura di), "Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea", Giappichelli, 2023

V. Salvatore (2023-b), *The regulatory challenges of digital therapeutics*, in "European Health & Pharmaceutical Law Review", 2023

V. Salvatore (2021), *Il diritto alla salute, una prospettiva di diritto comparato*, in "EPRS | Servizio Ricerca del Parlamento europeo", 2021

F. Scialoia (2024), *Verso la costruzione di un quadro regolatorio europeo sulle terapie digitali: sfide e opportunità*, in "Corti Supreme e Salute", 2024

F. Scialoia (2023), *L'Unione europea apre la strada alla creazione dello spazio europeo dei dati sanitari*, in V. Salvatore (a cura di), "Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea", Giappichelli, 2023

G. Simone (2020), *Machine Learning e tutela della Privacy alla luce del GDPR*, in G. Alpa (a cura di), "Diritto e intelligenza artificiale", Pacini Editore, 2020

J. Van Oirschot, G. Ooms (2022), *Interpreting the EU Artificial Intelligence Act for the Health Sector*, in "Health Action International", 2022

E.-B. Van Veen (2018), *Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate*, in "European Journal of Cancer", 2018

A. Volpato (2024), *Il ruolo delle norme armonizzate nell'attuazione del regolamento sull'intelligenza artificiale*, in "Quaderni AISDUE", 2024

W. Wiewiórowski (2021), *Synthetic data: what use cases as a privacy enhancing technology?*, in "European Data Protection Supervisor", 2021

G. Zaccaroni (2024), *Intelligenza artificiale e principio democratico: riflessioni a margine dell'emersione di un quadro normativo europeo*, in "Quaderni AISDUE", 2024

RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

Autori del 2025

Rosanna Amato Istituto di Informatica Giuridica e Sistemi Giudiziari – CNR
Daniele Amoroso Università degli Studi di Cagliari
Francesca Bailo Università di Genova
Nicola Pierpaolo Barbuzzi Universitas Mercatorum – Roma
Giovanni Barozzi Reggiani Università di Sassari
Marco Bombardelli Università di Trento
Lidia Bonifati Università Commerciale "Luigi Bocconi"
Fabio Bravo Università di Bologna
Raffaella Brighi Università di Bologna
Elda Brogi European University Institute – Florence
Simone Calzolaio Università degli Studi di Macerata
Omar Caramaschi Università degli Studi di Genova
Roberta Carlini European University Institute – Florence
Pier Giorgio Chiara Università di Bologna
Enza Cirone Università degli Studi di Firenze
Alfonso Contaldo Sapienza – Università di Roma
Fabrizio Corona Università di Brescia e LUISS Guido Carli
Stefano Corso Università di Padova
Antonio Cremone Università degli Studi di Firenze
Paola D'Abbrunzo Ministero dell'Istruzione e del Merito
Arcangelo Leone De Castris Alan Turing Institute – Londra
Ercole De Luca Areti S.p.a.
María Dolores García Sánchez University of Seville – Spain
Jan Erik Kermer European University Institute – Florence
Matteo Falcone Università degli Studi di Perugia
Elio Fameli già Istituto di Informatica Giuridica e Sistemi Giudiziari – CNR
Anxhela Ferhataj University of Tirana
Moreno Ferrarese Università di Trento
Chiara Fioravanti Istituto di Informatica Giuridica e Sistemi Giudiziari – CNR
Gaia Fiorinelli Scuola Superiore Sant'Anna di Pisa
Gino Fontana avvocato
Simone Franca Università di Trento
Fabio Francario Università degli studi di Siena
Michele Francaviglia Università degli Studi di Genova
Marco Guerra Università degli Studi Roma Tre
Elira Hoxha University of Tirana
Antonio Iannuzzi Università degli Studi Roma Tre
Ernesto Ingenito avvocato
José Osvaldo Ledesma Universidad Nacional del Nordeste – Argentina
Sara Lilli Scuola Superiore Sant'Anna di Pisa e Scuola IMT Alti Studi di Lucca
Camilla Lobascio Università degli Studi di Macerata
Luisa Lodevole Università degli Studi di Roma Tor Vergata
Erik Longo Università degli Studi di Firenze
Christiane Maaß University of Hildesheim – Germany and Research Centre for Easy Language
Indra Macrì Corte costituzionale
Alessandro Malacarne Università degli Studi di Genova
Luigi Malferrari University of Saarland and University of Strasbourg
Alessandro Manfredi Università Magna Græcia – Catanzaro
Antonio Manganelli Università degli Studi di Siena
Leonardo Marchesin Tribunale Ordinario di Venezia
Massimiliano Marletta Università di Catania
Teresa Meccariello Università degli Studi Federico II – Napoli
Francesco Midiri Università Cattolica del Sacro Cuore – Milano
Veronica Montozzi Università degli Studi di Roma Tre
Geordie Morciano Legal innovation specialist
Gaetana Morgante Scuola Superiore Sant'Anna di Pisa
Lorenzo Moroni Università di Cagliari
Nasir Muftić University of Sarajevo
Elisa Orrù Max Planck Institute for the Study of Crime, Security and Law – Freiburg and Freiburg University
Paolo Passaglia Università degli Studi di Pisa
Maria Chiara Pollicino Università degli Studi di Perugia
Benedetto Ponti Università degli Studi di Perugia
Marco Prandini Università di Bologna
Alberto Quintavalla Erasmus University – Rotterdam and Erasmus Center of Law and Digitalization
Dario Saul Navarro Universidad Nacional del Nordeste – Argentina
Federica Scialoia Università di Napoli "Parthenope"
Anna Simonati Università di Trento
Matteo Trevisan European University Institute – Florence
Pasquale Troncone Università degli Studi Federico II – Napoli
Alessandro Vannini Università di Bologna
Sofia Verza European University Institute – Florence
Maria Vittoria Zucca Scuola Superiore Sant'Anna di Pisa e Scuola IMT Alti Studi di Lucca
Kreshnik Vukatana University of Tirana
Paolo Zuddas Università degli Studi dell'Insubria